INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL GENERAL

2020/2021

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

A DEFESA NACIONAL NA PREVENÇÃO E COMBATE ÀS AMEAÇAS HÍBRIDAS

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

António José Ruivo Grilo

Coronel de Artilharia

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A DEFESA NACIONAL NA PREVENÇÃO E COMBATE ÀS AMEAÇAS HÍBRIDAS

COR ART António José Ruivo Grilo

Trabalho de Investigação Individual do CPOG 2020/2021

Pedrouços 2021

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A DEFESA NACIONAL NA PREVENÇÃO E COMBATE ÀS AMEAÇAS HÍBRIDAS

COR ART António José Ruivo Grilo

Trabalho de Investigação Individual do CPOG 2020/2021

Orientador: CMG FZ Artur José Figueiredo Mariano Alves

Pedrouços 2021

Declaração de compromisso Antiplágio

Eu, **António José Ruivo Grilo**, declaro por minha honra que o documento intitulado "**A Defesa Nacional na prevenção e combate às ameaças híbridas**" corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **Curso de Promoção a Oficial General 2020-2021** no Instituto Universitário Militar, e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, 07 de maio de 2021

Assinado por : **ANTÓNIO JOSÉ RUIVO GRILO**
Num. de Identificação: 07362861
Data: 2021.07.05 22:32:04+01'00'

António José Ruivo Grilo
Coronel de Artilharia

Agradecimentos

Os primeiros agradecimentos são dirigidos ao meu orientador, CMG FZ Artur José Figueiredo Mariano Alves, pela sua amizade, permanente disponibilidade, apoio na conceção e desenvolvimento do trabalho de investigação individual e pelas oportunas sugestões e contribuições.

Ao Tenente-Coronel Silva Costa, do Instituto Universitário Militar, pelos seus contributos e sugestões, no âmbito da metodologia de investigação científica, que muito ajudaram na conceção e elaboração da investigação.

Aos entrevistados que através da partilha da sua experiência, saber e reflexões, constituíram uma mais-valia e possibilitaram a realização deste trabalho.

Agradeço de forma especial a disponibilidade e apoio do Dr. Jorge Aranda, ao possibilitar uma partilha de conhecimento que, muito contribuiu para o desenvolvimento do tema.

Uma referência especial ao Major Lourenço Serrão, grande camarada e amigo, pelas críticas e desafios que me permitiram dar um rumo à investigação.

Aos camaradas auditores do Curso de Promoção a Oficial General 2020-2021, pela camaradagem insigne, partilha de conhecimentos e pelo apoio permanente manifestado ao longo do curso.

À minha família, pela sua disponibilidade, compreensão e incondicional apoio com que sempre posso contar.

A todos o meu obrigado.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Resumo

O atual ambiente estratégico é caracterizado pelo aparecimento de ameaças de natureza difusa e híbrida, potenciadas pela interconetividade e informatização da vida moderna, que visam explorar as vulnerabilidades de um país e, muitas vezes minar os valores democráticos, o que tem criado novos desafios no âmbito da Segurança e Defesa.

A compreensão das Ameaças Híbridas e, consequentemente, a capacidade de prevenção e combate a este fenómeno, passa obrigatoriamente pela implementação de uma estratégia multidimensional, caracterizada por ações coordenadas de uma abordagem compreensiva da Defesa Nacional e de uma resposta integrada de toda a sociedade.

O objeto do estudo é a Defesa Nacional face às Ameaças Híbridas, numa abordagem *whole of government* e *whole of society*, no âmbito nacional e dos compromissos assumidos com as organizações que integramos e, através das sinergias da União Europeia no campo da Ameaça Híbrida.

Neste contexto, adotou-se uma investigação baseada num raciocínio indutivo, de estratégia qualitativa e desenho de pesquisa de estudo de caso.

Como principais resultados, identificámos as Ameaças Híbridas consideradas mais prováveis e críticas a Portugal e, para as quais, em face da análise do ambiente externo e do ambiente interno, concluímos uma proposta de 21 linhas de ação estratégicas para apropriar o País na prevenção e combate às Ameaças Híbridas, nomeadamente ao nível da Defesa Nacional num conceito alargado de Segurança e Defesa.

Palavras-chave:

Ameaças Híbridas, Combate às Ameaças Híbridas, Defesa Nacional.

Abstract

The current strategic environment is characterized by the emergence of threats of diffuse and hybrid nature, enhanced by the interconnectivity and computerization of modern life, which aim to exploit the vulnerabilities of a country and often undermine democratic values, which has created new challenges in the field of Security and Defense.

The understanding of Hybrid Threats and, consequently, the ability to prevent and combat this phenomenon, necessarily involves the implementation of a multidimensional strategy, characterized by coordinated actions of a comprehensive approach of National Defense and an integrated response from the whole society.

The object of the study is the National Defense in the face of Hybrid Threats, in a whole of government and whole of society approach, within the national scope and the commitments assumed with the organizations we integrate, and through the synergies of the European Union in the field of the Hybrid Threat.

In this context, we adopted a research based on an inductive reasoning, qualitative strategy, and case study research design.

As main results, we identified the Hybrid Threats considered most likely and critical to Portugal and, for which, in view of the analysis of the external and internal environment, we concluded a proposal of 21 strategic lines of action to appropriate the country in preventing and combating Hybrid Threats, namely at the level of National Defense in a broad concept of Security and Defense.

Keywords:

Counter Hybrid Threats, Hybrid Threats, National Defense.

Lista de abreviaturas, siglas e acrónimos

AH	Ameaças Híbridas
AR	Assembleia da República
CAH	Combate de Ameaças Híbridas
CEDN	Conceito Estratégico de Defesa Nacional
CoG	Centros de Gravidade
CPDN	Ciclo de Planeamento de Defesa Militar
CPOG	Curso de Promoção a Oficial General
DN	Defesa Nacional
EM	Estados-Membros
FFAA	Forças Armadas
GAO	*Government Accountability Office*
GH	Guerra Híbrida
IA	Inteligência Artificial
IUM	Instituto Universitário Militar
LA	Linha de Ação
LAE	Linha de Ação Estratégica
LDN	Lei de Defesa Nacional
MC	*Military Committee*
MCDC	*Multinational Capability Development Campaign*
MDN	Ministério da Defesa Nacional
MIFA	Missões das Forças Armadas
MPECI	Instrumentos de poder militar, político, económico, civil e informacional
NATO	Organização do Tratado do Atlântico Norte
NDPP	*NATO Defence Planning Process*
NEP	Normas de Execução Permanente

OE	Objetivo específico
OG	Objetivo geral
PI	Projeto de Investigação
PMESII	Vulnerabilidades política, militar, económica, social, informacional e de infraestruturas
PPUE	Presidência Portuguesa da UE
QC	Questão central
QD	Questão derivada
SSI	Sistema de Segurança Interna
SWOT	*Strengths, Weaknesses, Opportunities e Threats* (respetivamente, Potencialidades, Vulnerabilidades, Oportunidades e Ameaças)
TII	Trabalho de Investigação Individual
UE	União Europeia
US	*United States*

1. Introdução

As Ameaças Híbridas (AH) e a Guerra Híbrida (GH) são conceitos que ganham expressão com os acontecimentos na Ucrânia em 2014, em que a Rússia desenvolveu ações sincronizadas, recorrendo aos diversos instrumentos de poder, de forma a explorar as vulnerabilidades dos seus adversários e a alcançar os seus objetivos políticos. Em consequência, a Organização do Tratado do Atlântico Norte (NATO) classificou tais ações como híbridas (Fernandes, 2016) e viria a referir-se, formalmente, ao termo "ameaças de guerra híbrida"[1], para caracterizar as ameaças aos países da Aliança no século XXI (North Atlantic Treaty Organization [NATO], 2014).

O atual ambiente operacional possibilita às AH a utilização de uma grande diversidade de métodos e atividades, incluindo a desinformação, a exploração da tendência crescente de dependência energética, os transportes, a chantagem económica, a pressão diplomática, o minar das instituições internacionais, o terrorismo, o crime organizado, as tecnologias disruptivas exponenciadas pelo domínio Ciber, resultando no aumento da insegurança. Em oposição ao conceito de *Military Centric Warfare* que se ancora no domínio militar, a GH procura orquestrar ações nos mais diversos domínios e usa a plasticidade e a dinâmica, para criar ambiguidade (*Countering Hybrid Threats Centre of Excellence* [Hybrid CoE], 2017).

Apesar dos conceitos de AH e GH não serem novidade, a revolução digital, iniciada no século passado, veio redimensioná-los. A dependência do armazenamento de informação, a análise integrada de dados, os avanços na inteligência artificial (IA) e a acessibilidade globalizada às tecnologias emergentes, são e serão, oportunidades de desenvolvimento nos diversos domínios, mas também riscos por potenciarem as AH (Ralph, 2016).

O combate das AH constitui, assim, um desafio, porque estas vivem no foro da impossibilidade de deteção imediata e usam elementos caracterizadores de *soft*, *hard* e *smart power*, atuando numa *Grey Zone* com limites difusos e mal definidos, para manipular a população e corroer os governos e as sociedades, criando *stress* nos processos de decisão dos Estados democráticos (Hybrid CoE, 2017), através da erosão da confiança publica nas instituições governamentais e do ataque aos valores fundamentais da sociedade (Comissão Europeia, 2018).

[1] Na Declaração Final da Cimeira da NATO de 2014.

É no contexto deste novo paradigma civilizacional, com desafios em termos de defesa e segurança, que as AH têm prosperado pelo potencial perturbador que trazem aos Estados de direito democrático (Pereira, 2018).

O assunto passou a ser prioridade nas agendas da União Europeia (UE)[2] e da NATO, que apresentam um conjunto de linhas de ação e medidas de forma a assegurar aos Estados-Membros (EM), uma base forte que os apoie na luta coletiva contra as AH, alicerçada na colaboração interinstitucional (Comissão Europeia, 2016a). Resalvando a manutenção da responsabilidade primária dos EM para fazer face à AH, que deverão aumentar a sua resiliência, a fim de mitigar as vulnerabilidades nacionais que são específicas (Comissão Europeia, 2016a).

Ao nível da documentação estratégica nacional não há, ainda, referência às AH. Contudo, as declarações da ex-Secretária de Estado da Defesa Nacional, Ana Santos Pinto, por ocasião da candidatura de Portugal a membro do Centro Europeu de Excelência para Combate de Ameaças Híbridas (CAH) (Hybrid CoE)[3], foram reveladoras da preocupação do governo no CAH. Declarou, então, que a adesão "*Resulta de um processo nacional, de reconhecimento que as AH são uma prioridade…*", acrescentando que são questões "*transversais a várias áreas do Governo*" (LUSA, 2019).

Mais recentemente, são ainda evidências da relevância e atualidade nacional do tema, o seminário sobre a importância das AH à segurança, realizado em março de 2021, organizado pela presidência portuguesa do Concelho da UE, bem como a elaboração do documento de enquadramento nacional das AH, orientado segundo uma abordagem *whole of government*, com uma perspetiva conjunta e interministerial sobre a posição de Portugal, procurando projetar os interesses nacionais em matéria de combate de AH e como potenciar a participação nacional nas organizações internacionais.

Assim, este TII revela-se de elevada importância e acuidade, pela necessidade de reflexão sobre as linhas de ação em matéria de Defesa Nacional (DN), numa abordagem abrangente e fazendo a desconstrução conceptual da GH e da AH, para acomodar as principais linhas de orientação da UE e as sinergias criadas no âmbito da UE e da NATO.

O objeto do estudo é a DN face às AH, no contexto nacional e no âmbito dos compromissos assumidos com as organizações que integra (UE e NATO).

[2] A UE através da Comissão Europeia e do Serviço Europeu para Ação Externa (EEAS) desenvolveram, em 2016, medidas para aumentar a resiliência dos seus EM.
[3] A 29 agosto de 2019.

Atendendo à abrangência do tema, o trabalho foi delimitado nos seguintes âmbitos: tempo, conteúdo e espaço.

Em termos temporais, a investigação abrange o período a partir de 2016 por representar uma clara definição política da UE no CAH.

A investigação é delimitada ao nível do conteúdo na AH e nas medidas de orientação da UE para o CAH que tenham implicações nacionais.

No domínio espacial, delimita-se este estudo à recolha de informação tendo em conta o Espaço Estratégico de Interesse Nacional Permanente e, as prioridades da política externa e da DN no âmbito da UE e da NATO.

Com a finalidade de orientar o trabalho de investigação, foram formulados como objetivos de investigação, um objetivo geral (OG) e três objetivos específicos (OE): OG: Propor linhas de ação estratégicas no âmbito da Defesa Nacional para o Combate às Ameaças Híbridas; OE 1: Analisar o papel da Defesa Nacional no Combate às Ameaças Híbridas; OE2: Analisar o ambiente externo face às Ameaças Híbridas; OE3: Analisar o ambiente interno face às Ameaças Híbridas.

Assim, definimos uma Questão Central (QC) e três Questões Derivadas (QD): QC: Quais são as principais linhas de ação estratégicas para o Combate às Ameaças Híbridas ao nível da Defesa Nacional?; QD 1: Qual é o papel da Defesa Nacional no Combate às Ameaças Híbridas?; QD 2: Quais as principais ameaças e oportunidades da Defesa Nacional face às Ameaças Híbridas?; QD 3: Quais as principais potencialidades e vulnerabilidades da Defesa Nacional face às Ameaças Híbridas?.

Para a sua realização adotou-se uma investigação baseada num raciocínio indutivo, a metodologia seguiu a estratégia de investigação qualitativa e um desenho de estudo de caso, recorrendo à análise documental e a entrevistas semiestruturadas, como instrumentos de recolha de dados e à análise de conteúdo e análise SWOT - *Strengths, Weaknesses, Opportunities e Threats* (respetivamente, Potencialidades, Vulnerabilidades, Oportunidades e Ameaças) como técnicas de tratamento de dados.

O trabalho de investigação é organizado em oito capítulos.

No primeiro capítulo, da introdução, será apresentado o enquadramento e justificação da investigação, o objeto da investigação e sua delimitação, os objetivos e as questões centrais e gerais da investigação e, a organização geral da investigação.

No segundo capítulo, do enquadramento teórico e conceptual, será apresentada a revisão da literatura, com a finalidade de contextualizar e conceptualizar a temática das AH.

No terceiro capítulo, da metodologia e do método, aborda-se o percurso metodológico nas suas diferentes fases, o raciocínio, a estratégia de investigação e desenho de pesquisa, os instrumentos e as técnicas de recolha, análise e tratamento de dados.

No quarto capítulo, do papel da DN no CAH, será feita a análise da DN para fazer face à AH, nomeadamente através dos domínios de poder, permitindo o desenvolvimento do OE 1 e a resposta à QD1.

No quinto capítulo, será apresentada a análise das medidas de CAH através de dados provenientes da organização de referência (quadro da UE) e pela análise das entrevistas semiestruturadas, identificando-se as principais ameaças e oportunidades para a DN no CAH, no ambiente externo, possibilitando cumprir o OE2 e responder à QD2.

No sexto capítulo, vai proceder-se à análise das vulnerabilidades e potencialidades, no ambiente interno, alcançando-se o OE3, para responder à QD3.

No sétimo capítulo, recorrendo à análise de Matrizes SWOT e, com base em critérios de adequabilidade, aceitabilidade e exequibilidade, responde-se à QC, propondo-se as linhas de ação estratégicas para o Combate às AH.

No oitavo capítulo, das conclusões apresenta-se um breve enquadramento do trabalho, um sumário do procedimento metodológico seguido, uma súmula dos resultados obtidos e dos contributos para o conhecimento, as limitações e, sugestões para pesquisas futuras.

2. Enquadramento teórico e conceptual

Neste capítulo pretende-se, inicialmente, apresentar a evolução do conceito das AH e GH e os seus contextos de aplicação. Após esse enquadramento, com o corpo de conceitos desenvolvidos em Apêndices A e B, desconstruímos o conceito de AH, perscrutando a sua evolução e identificando o que o diferencia de outros termos comuns na fraseologia sobre os conflitos. Seguidamente, percorremos os trabalhos ao nível da NATO e UE para, como corolário, atender ao despertar nacional, revigorado no contexto da Presidência Portuguesa da UE (PPUE).

2.1 Estado da arte e revisão de literatura

A dificuldade na definição concetual das AH e GH tem limitado o seu entendimento internacional, existindo inclusive fortes divergências na interpretação do fenómeno, nas suas origens, bem como, na sua tipologia e forma de as combater. Um dos principais problemas de conceptualização tem a ver com a linguagem, existindo na literatura especializada uma panóplia de termos relacionados com esta temática, que são usados de forma indiscriminada sem definição consensual (AH, GH, conflito híbrido, influência híbrida, ataque híbrido, zona híbrida ou cinzenta). Nesse sentido, importa para a clareza concetual necessária, definir e distinguir os diferentes conceitos dentro de uma abordagem abrangente de segurança nacional (*Multinational Capability Development Campaign* [MCDC][4], 2019) e para o qual contribui o corpo de conceitos em Apêndice A.

Desta forma, o foco será o conceito de AH por enformar toda a investigação que percorre o quadro científico que sustente a apresentação final, de linhas de ação. Porém, o suporte assegurado pela compreensão do conceito de GH (Apêndice B) garante um claro entendimento das diferenças conceptuais que convém atentar.

2.1.1 O elemento diferenciador das Ameaças Híbridas e suas manifestações

Tendo em conta a realidade que AH e GH correspondem a diferentes desafios à segurança nacional, o MCDC (2019), vem distinguir os dois conceitos. Para esta organização, as AH combinam uma ampla gama de meios não violentos para visar vulnerabilidades em toda a sociedade, a fim de minar o funcionamento, a unidade ou a vontade de seus alvos, degradando e subvertendo o *status quo,* sendo que este tipo de

[4] *MCDC Countering Hybrid Warfare* foi um projeto que decorreu de jun17 a dez18 e incluiu 14 nações (Áustria, Canada, República Checa, Dinamarca, Alemanha, Espanha, Finlândia, Reino Unido, Noruega, Holanda, Polonia, República da Coreia, Suíça e Estados Unidos) e, envolveu a UE, a NATO e o Hybrid CoE.

estratégia é usado para atingir gradualmente os objetivos dos perpetradores sem desencadear respostas decisivas, incluindo armadas. Em contraponto, a GH, consiste no desafio apresentado pela crescente complexidade do conflito armado, em que os adversários podem combinar diferentes tipos de guerra com meios não militares para neutralizar o poder militar convencional (MCDC, 2019).

Este posicionamento, apresentado na Figura 1, de distinção conceptual das AH em relação à GH durante as diferentes fases de um conflito, sustenta que as AH podem ter lugar sem nunca se chegar à GH e ao confronto direto.

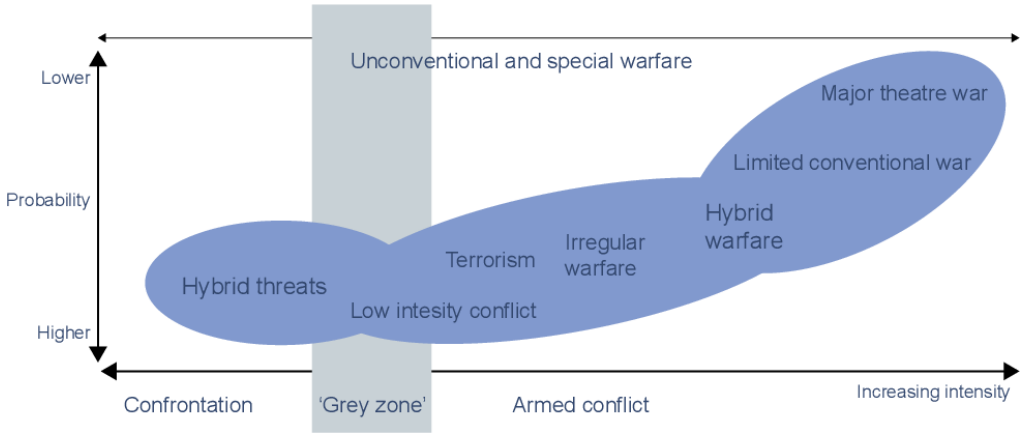

Figura 1 - Ameaças Híbridas vs Guerra Híbrida
Fonte: MCDC (2019), p. 4.

Presentemente, a NATO possui uma Estratégia de CAH embora se centre fundamentalmente nas estratégias da GH fruto da sua vocação, motivo pelo qual o estudo se orienta para a UE mais centrada com a AH e o CAH, que desenvolveu um manual de instruções para combater AH[5] e criou, em Helsínquia, em 2017[6] um Hybrid Fusion Cell[7] e o Hybrid CoE (Pereira, 2018).

No âmbito da concetualização das AH, estas podem manifestar-se de diversas formas e em diferentes domínios, abrangendo "[…] desde as campanhas mediáticas à utilização de armas químicas, biológicas, radiológicas e nucleares, passando por ciberataques contra os sistemas informáticos de infraestruturas estratégicas ou pela utilização de meios de subversão da paz social ou da ordem económica" (Pereira, 2018, p. 11).

[5] Hybrid CoE (2020), *The Landscape of Hybrid Threats: A Conceptual Model*.
[6] UE inaugura o *European Centre of Excellence for Countering Hybrid Threats*, 02Out17, www.hybridcoe.
[7] Vocacionado para recolha, processamento e análise de informações.

Segundo o MCDC (2019), as AH manifestam-se através de uma diversidade de tipologias de instrumentos expostas na Figura 2, forçosamente combinados (Alves, 2020) e podendo associar-se a uma variedade de cenários de guerra.

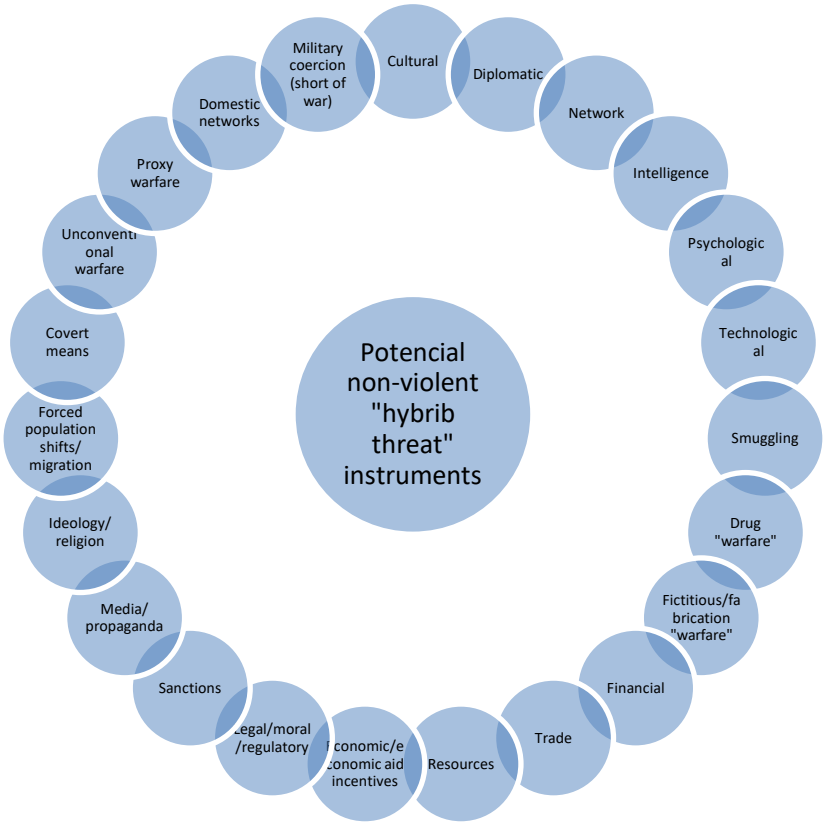

Figura 2 – Tipologia de instrumentos das Ameaças Híbridas

Fonte: Adaptado de Monaghan (2019), p.5.

Sendo executadas "[…] quando um ator combina e sincroniza ações de forma deliberada, para atingir as vulnerabilidades sistémicas de sociedades democráticas, recorrendo a formas de atuação dos estados autoritários e outros atores para enfraquecer os sistemas democráticos" (Giannopoulos & Smith, 2019, p.4).

2.1.2 Linhas de ação da UE para o Combate de Ameaças Híbridas

Para a UE, a instabilidade nas regiões que lhe são confinantes e a evolução ao nível das ameaças, motiva um crescente número de desafios que se colocam em questões de paz, segurança e prosperidade. Assim o Presidente da Comissão Europeia, Jean-Claude Juncker salientou, nas suas orientações políticas de 2014, a necessidade de reforçar a Europa em assuntos de segurança e de defesa, enformando o que viria a ser um quadro conjunto com propostas para fazer face às AH e reforçar a resiliência da UE.

Nesse sentido, a Comissão Europeia e o Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, propuseram em abril de 2016 a adoção de

um quadro comum com vinte e duas ações operacionais sustentado em 4 domínios estratégicos prioritários: (i) aumentar o conhecimento da situação; (ii) reforçar a resiliência; (iii) reforçar a capacidade dos EM e da União para prevenir e dar resposta às crises e para recuperar de forma coordenada e; (iv) reforçar a cooperação com a NATO a fim de assegurar a complementaridade das medidas (Comissão Europeia, 2016b).

Pretende este quadro dar aos EM uma base que os apoie na luta coletiva contra as AH, apoiado por instrumentos e iniciativas da UE e utilizando todo o potencial dos Tratados (Comissão Europeia, 2016b).

Mais recentemente, em junho de 2018, o Alto Representante da UE para os Negócios Estrangeiros e a Política de Segurança, em conjunto com a Comissão Europeia, publicaram uma comunicação conjunta, na qual ficaram definidas as principais linhas de orientação para CAH (Comissão Europeia, 2018).

Esta declaração realça a preocupação que estes desafios apresentam, mas também mostram que a capacidade de resposta deve ser combinada. Defendem assim, que o CAH deve assentar nos seguintes pilares: i) consciência situacional, tendo a UE criado, em 2017, o Hybrid Fusion Cell, que funciona no âmbito do UE Intelligence and Situation Centre Structure e do Serviço Europeu de Ação Externa, com a missão de recolha, processamento e análise de informações sobre as AH; ii) comunicação estratégica, sendo que um dos vetores de potencial sucesso das AH reside na falta de comunicação e no isolamento dos países visados; iii) reforçar a resiliência e capacidade de contenção no setor da cibersegurança, tendo proposto a criação de um certificado de cibersegurança, o reforço das competências da Agência Europeia para a Cibersegurança, um quadro reforçado de cooperação entre EM e a UE em caso de ciberataque, bem como o conjunto de instrumentos de ciberdiplomacia e; iv) reforçar a resiliência perante atividades hostis de espionagem pretendendo, neste âmbito, melhorar a capacidade do UE Hybrid Fusion Cell no campo da contraespionagem (Pereira, 2018).

Um modelo conceptual[8], é desenvolvido pela UE em dezembro de 2019, para apoio das Nações na definição estratégias nacionais para o combate às AH., salientado atores, domínios e ferramentas e, sistematizando as bases para um plano adaptável às necessidades de cada EM da UE e da NATO (Hybrid CoE, 2020).

[8] Hybrid CoE (2020), *The Landscape of Hybrid Threats: A Conceptual Model*.

Neste contexto, o Hybrid CoE, sustenta que a comunicação conjunta da Comissão Europeia sobre AH, publicada em 2016, centra-se numa série de ações de nível operacional e que, por sua vez, a comunicação conjunta de 2018, fornece uma visão mais estratégica sobre o tema, claramente delineando a importância dos aspetos estratégicos como o reforço da resiliência (Giannopoulos & Smith, 2019).

2.1.3 Portugal e o conceito de Ameaças Híbridas

Entre um de janeiro e 30 de junho de 2021, Portugal assume a Presidência rotativa do Conselho da UE. O programa da Presidência assenta como principais prioridades expressas na Agenda Estratégica 2019-2024, a proteção dos cidadãos e das liberdades; o desenvolvimento de uma base económica forte e dinâmica; a construção de uma Europa com impacto neutro no clima, mais verde, mais justa e social e; a promoção dos interesses e valores europeus, (Comissão Europeia, 2020).

No âmbito da Política Comum de Segurança e Defesa, realça-se que a capacidade de agir da UE, depende do que queremos ser capazes de fazer enquanto europeus. A análise das ameaças constituirá a base para o diálogo estratégico que contribua para um entendimento político comum e um plano de desenvolvimento de capacidades de defesa. O reforço da coesão e da capacidade de ação conjunta da NATO e da UE deverá incluir a defesa, a cibersegurança, bem como as AH" (Comissão Europeia, 2020).

Neste âmbito da PPUE, realça-se a importância das AH, sendo reflexo disso o seminário intitulado "A importância das AH à segurança, na vizinhança sul da Europa", realizado em março de 2021, organizado pela PPUE, pelo Ministério dos Negócios Estrangeiros (MNE) e pelo Hybrid CoE. Posteriormente, em abril de 2021, no seminário "AH, incluindo desinformação", organizado pelo MNE e pelo Serviço de Informações e Segurança, o Ministro dos Negócios Estrangeiros Augusto Santos Silva, alertou para as campanhas de desinformação, influência e interferência, patrocinados por rivais sistémicos da Europa, referindo-se a atores híbridos. Salienta-se ainda a constituição de um grupo de trabalho, liderado pelo MNE, de redação do documento de enquadramento nacional para fazer face às AH que, no fundo, constituirá a estratégia nacional de CAH.

2.2 Modelo de Análise

Este tema insere-se no Domínio das Ciências Militares e, enquadra-se, no âmbito da Área de Investigação das Operações Militares e do Estudo das Crises e Conflitos Armados

(Decreto-Lei n.º 249, 2015), nas subáreas do Planeamento Operacional e no Planeamento Estratégico Militar.

Para além de artigos e trabalhos de investigação, de autores nacionais, utilizam-se, fontes bibliográficas de autores de origem americana e de países aliados, fundamentalmente da UE.

A dificuldade na definição concetual das AH e GH tem limitado o seu entendimento internacional, existindo divergências na sua interpretação, pelo que importa clarificar que esta investigação se foca nas AH, aproveitando fundamentalmente as sinergias da UE.

O Quadro 1 ilustra o Modelo de Análise.

Quadro 1 - Modelo de Análise

<table>
<tr><td>OBJETIVO GERAL</td><td colspan="6">Propor linhas de ação estratégicas no âmbito da Defesa Nacional para o CAH.</td></tr>
<tr><td rowspan="2">OBJETIVOS ESPECIFICOS</td><td>QUESTÃO CENTRAL</td><td colspan="5">Quais são as principais linhas de ação estratégicas para o CAH ao nível da Defesa Nacional?</td></tr>
<tr><td>QUESTÕES DERIVADAS</td><td>CONCEITOS</td><td>DIMENSÕES</td><td>INDICADORES</td><td>INSTRUMENTOS DE RECOLHA E TÉCNICAS DE TRATAMENTO DE DADOS</td><td>CRITÉRIOS DE AVALIAÇÃO</td></tr>
<tr><td>OE 1
Analisar o papel da Defesa Nacional no CAH.</td><td>QD 1
Qual é o papel da Defesa Nacional no CAH?</td><td rowspan="3">AH

CAH

Defesa Nacional

Instrumentos de Poder e Domínios

Tipologia das AH</td><td>Funções críticas PMESII

Ciberespaço</td><td>Domínios
Whole of society</td><td>Análise documental</td><td rowspan="3">Entrevistas Confirmação
Adequabilidade
Aceitabilidade
Exequibilidade</td></tr>
<tr><td>OE 2
Analisar o ambiente externo face à AH.</td><td>QD 2
Quais principais ameaças e oportunidades da DN face à AH?</td><td>Conhecimento Situacional

Comunicação Estratégica

Resiliência</td><td>Ameaças

Oportunidades</td><td>Análise documental e entrevistas semiestruturadas

Análise de conteúdo e análise SWOT</td></tr>
<tr><td>OE 3
Analisar o ambiente interno face à AH.</td><td>QD 3
Quais as principais potencialidades e vulnerabilidades da DN face à AH?</td><td>Prevenção e resposta a crises</td><td>Potencialidades

Vulnerabilidades</td><td>Análise documental e entrevistas semiestruturadas

Análise de conteúdo e análise SWOT</td></tr>
</table>

3. Metodologia e método

Neste capítulo, inscreve-se a metodologia de investigação e o método utilizado nos instrumentos de recolha e técnicas de tratamento de dados.

3.1 Metodologia

O presente trabalho, necessariamente de investigação aplicada porque pretende elaborar contributos diretos em face da pesquisa realizada, seguirá as orientações metodológicas do Instituto Universitário Militar (IUM), tendo ainda como referências as Normas de Execução Permanente (NEP) aprovadas, INV 001 (NEP/INV-001 (A1), 2020a) e INV 003 (NEP/INV-001 (A1), 2020b).

Para a abordagem metodológica deste tema, adota-se a posição ontológica construtivista, que considera que os fenómenos sociais e os seus significados são produzidos com base nas interações entre atores sociais e entre estes e a envolvente, pelo que estão em constante revisão (Bryman, 2012), e epistemológica interpretativa, que advoga que o mundo social, ao ser formado por indivíduos e pelas suas interações, não pode, nem deve ser estudado a partir dos princípios, ferramentas e técnicas das ciências naturais, competindo ao investigador não só verificar os fenómenos, mas também compreender os significados subjetivos desses mesmos fenómenos (Bryman, 2012).

Baseada num raciocínio indutivo, a metodologia segue a estratégia de investigação qualitativa e um desenho de pesquisa de estudo de caso, pela recolha de informação detalhada sobre uma unidade de estudo e análise de variação (Santos e Lima, 2019).

A Figura 3 apresenta o método de investigação e as opções seguidas.

Figura 3 - Metodologia de Investigação
Fonte: Adaptado de Saunders (2009), citado por Santos e Lima (2019)

O percurso metodológico integrou duas fases, tendo a 1ª Fase terminado com a entrega e apresentação do projeto de investigação e, a 2ª Fase, com a finalização do trabalho e a preparação para a apresentação e defesa (NEP/INV-001 (A1), 2020a).

A Figura 4 ilustra a estrutura de investigação.

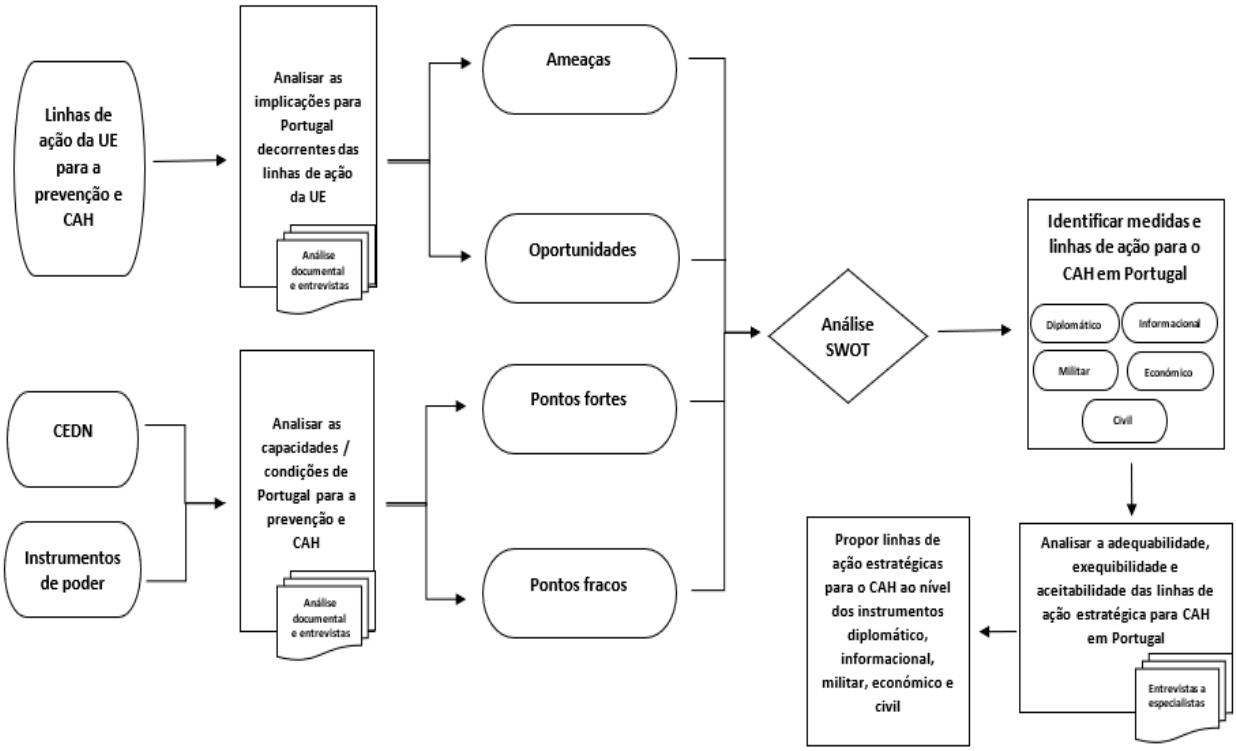

Figura 4 – Estrutura guia de investigação

3.2 Método

3.2.1 Participantes e procedimento

As entrevistas realizadas centraram-se na análise das áreas da defesa nacional do CAH. Constituíram-se em quatro entrevistas exploratórias, numa primeira fase, e, posteriormente, em profundidade numa fase mais avançada 17 entrevistas[9] dirigidas a personalidades especialistas na matéria, recorrendo à plataforma de vídeo conferência TEAMS e por email, no período de novembro a março, conforme Apêndice E.

As entrevistas que se constituem como uma amostra do tipo não probabilística ou empírica, intencional (Santos & Lima, 2019), foram estruturadas selecionando dois grupos

[9] Quantitativo enquadrado, inclusive por "excesso", na dimensão da amostra (N=12) de "informantes relativamente homogéneo", para um número de entrevistas que habitualmente permite obter saturação. (Rego, Cunha, & Meyer, 2019, p. 53).

de participantes. Um primeiro grupo de quatro entrevistas, a representantes de organismos centrais do estado e representantes dos diferentes instrumentos de poder que integram o grupo de trabalho liderado pelo MNE para a AH e, um segundo grupo de 13 entrevistas a estudiosos de reconhecida competência na matéria em estudo.

3.2.2 Instrumentos de recolha de dados

As técnicas de recolha de dados centraram-se na análise documental de fontes e origens diversas, recaindo prioritariamente nas áreas da defesa nacional, do CAH, complementada com entrevistas exploratórias, numa primeira fase e, posteriormente, entrevistas, do tipo semiestruturadas com recurso a tópicos e perguntas (Sarmento, 2013, p. 34), que recorreram a um guião (em Apêndice F) e dirigidas a personalidades especialistas na matéria com o objetivo de analisar opiniões sobre os diferentes domínios considerados pertinentes para a pesquisa (Fachada, et al., 2020).

3.2.3 Técnicas de tratamento dos dados

A análise de dados realizada de forma indutiva através da operacionalização de conceitos, onde as entrevistas semiestruturadas foram sujeitas a uma análise tipológica de conteúdo, para obter indicadores que permitiram inferência de conhecimentos (Fachada, et al., 2020).

A técnica de análise dos dados recolhidos é a análise categorial. Deste modo constituíram-se por questão, as unidades de contexto, determinam-se as unidades de registo e elabora-se o quadro com as unidades de contexto e registo. Seguidamente constrói-se o quadro com a análise conteúdo, onde se qualificam as unidades de registo pelas suas características comuns, as unidades de enumeração e se reagrupam em categorias (Sarmento, 2013, pp. 14-15 e 48-66).

Finda análise de conteúdo por categoriais efetuou-se a análise interpretativa de resultados (Santos & Lima, 2019), conforme Apêndice G.

Posteriormente analisou-se o ambiente externo e o ambiente interno para permitir através de cinco Matrizes SWOT (Apêndice H), para os domínios base das ameaças identificadas, analisar e apresentar os principais Objetivos Estratégicos e LA no CAH. As LA foram sujeitas a provas da estratégia, por validação por entrevistas de confirmação pelos critérios de adequabilidade, aceitabilidade e exequibilidade (Yarger 2006), finalizando-se com a proposta das LAE nacionais para o CAH.

4. O papel da Defesa Nacional no Combate de Ameaças Híbridas

As AH são foco de preocupação dos Estados de Direito Democrático, procurando-se uma resposta coletiva, participada e credível, através de uma abordagem compreensiva da Defesa Nacional e uma resposta integrada de toda a sociedade.

4.1 Instrumentos de poder

A DN tem por objetivos garantir a soberania do Estado, a independência nacional e a integridade territorial de Portugal. Visa assegurar a liberdade e a segurança das populações e a proteção dos valores fundamentais da ordem constitucional contra qualquer agressão ou ameaça externas, e assegura ainda o cumprimento dos compromissos internacionais, de acordo com o interesse nacional (Declaração de Retificação n.º 52/2009, de 20 de julho, à Lei n.º 31-A/2009, de 7 de Julho (2009)).

Salienta-se que para além da sua componente militar, a política de defesa nacional compreende as políticas sectoriais do Estado cujo contributo é necessário para a realização do interesse estratégico de Portugal e para o cumprimento dos objetivos da defesa nacional (Declaração de Retificação n.º 52/2009, de 20 de julho, à Lei n.º 31-A/2009, de 7 de Julho (2009)).

O Conceito Estratégico de Defesa Nacional (CEDN), que define os aspetos fundamentais da estratégia global a adotar pelo Estado para a consecução dos objetivos da política de segurança e defesa nacional (Resolução do Conselho de Ministros n.º 19, 2013), deixou de ser um confronto exclusivamente entre forças militares, para obrigar à mobilização de todos os recursos da nação, pelo que face ao espectro das ameaças para o Estado, os recursos económicos, políticos, tecnológicos e psicológicos, transformaram-se eles próprios em instrumentos de coação (Barroso, 2008).

Por sua vez a doutrina NATO, salienta que os instrumentos do poder emanam das fontes de poder e são um conjunto de capacidades que o Estado pode utilizar para executar as suas estratégias, sistematizados em: (i) diplomático; (ii) informacional; (iii) militar e (iv) económico)[10] *AJP-01* (2017).

A política de defesa nacional deve assim "[…] utilizar os instrumentos de poder político, económico, psicológico e militar de acordo com as diretivas políticas para criar os efeitos necessários à proteção dos interesses nacionais" (Yarger, 2006, p.1).

[10] Vulgarmente designados pelo seu acrónimo DIME.

O MCDC "*Countering Hybrid Warfare Project*", salienta que um ator estatal ou não-estatal, usa numa abordagem *whole of society* os seus instrumentos de poder militar, político, económico, civil e informacional (MPECI), que também designa como funções críticas, nas vulnerabilidades política, militar, económica, social, informacional e de infraestruturas (PMESII) do seu oponente, ilustrado na Figura 5 (MCDC, 2019).

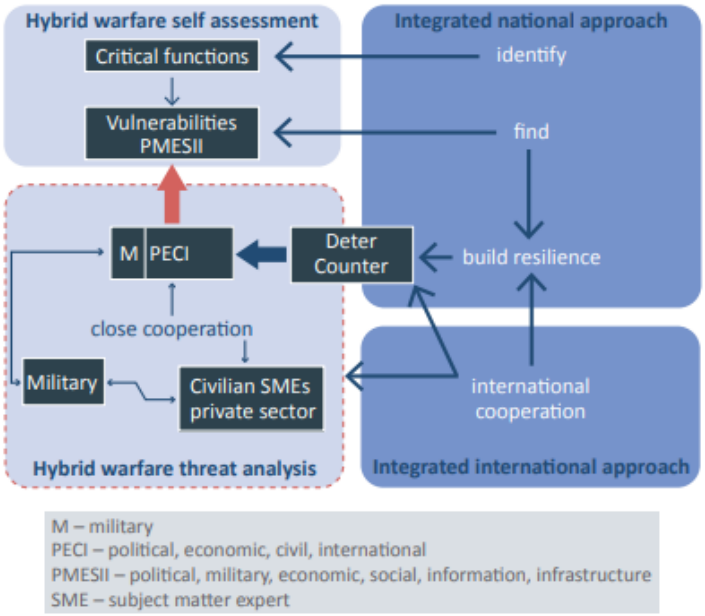

Figura 5 - Escalada da Guerra Híbrida
Fonte: MCDC (2017) p. 23.

A sua intensidade pode escalar verticalmente em intensidade e horizontalmente entre instrumentos de poder, para atingir os objetivos desejados (MCDC, 2019).

Finalmente, em dezembro de 2019[11], surge um modelo conceptual, desenvolvido pelo Hybrid CoE, para apoio das Nações na definição de estratégias nacionais para o CAH, que apresenta 13 domínios de poder e visa suprir as lacunas entre os domínios militar e civil e, ajudar a estabelecer uma base de entendimento comum e partilha entre civis e militares. De igual forma, pretende apoiar a conceção das ações certas para enfrentar as AH. A este respeito, refere-se que o modelo conceptual deve ser considerado como um ponto de referência para os decisores políticos, a fim de conceber políticas e ações eficazes e eficientes (Hybrid CoE, 2020).

Tendo a AH uma natureza adaptativa, que lhe possibilita prosperar no anonimato, sugere-se pensar na capacidade que os países têm para recuperar a estabilidade, apontando-

[11] Hybrid CoE (2020), *The Landscape of Hybrid Threats: A Conceptual Model*.

se mais ao conceito de resiliência, do que propriamente, identificar fraquezas passíveis de explorar (vulnerabilidades), pelo que o CAH inclui a sua prevenção[12](Giannopoulos & Smith, 2019).

4.2 Instrumentos de Poder e Domínios no Combate de Ameaças Híbridas

Considerando as diferentes abordagens aos instrumentos, funções críticas ou domínios de poder, sintetiza-se no Quadro 2 as diferentes abordagens anteriormente expostas:

Quadro 2 - Síntese de Instrumentos e Domínios de Poder

Fonte	Yarger	NATO	MCDC	Hybrid CoE UE
Instrumentos de Poder	Político		Político	Político
	Económico	Económico	Económico	Económico
	Psicológico			
	Militar	Militar	Militar	Militar e Defesa
		Diplomático		Diplomático
		Informacional	Informacional	Informacional
			Civil	
				Infraestruturas
				Ciber
				Espaço
				Cultural
				Administração Pública
				Legal
				Social
				Informações

Fonte: Adaptado de Yarger (2006), NATO (2017), MCDC (2019), Hybrid CoE (2019)

Apresentam-se em Apêndice C os conceitos associados aos domínios de poder do CAH, identificados no modelo conceptual do Hybrid CoE para o CAH. Este modelo procura fornecer os meios para abordar as vulnerabilidades, facilitar a deteção e fomentar a resiliência, adotando uma abordagem global que considera devidamente a prevenção, preparação, resposta e recuperação.

O atual espectro das ameaças para o Estado, nomeadamente a AH, obriga à mobilização de todos os recursos da nação, numa abordagem compreensiva e multidisciplinar da Defesa Nacional, englobando a Segurança e Defesa de modo holístico. Com este enquadramento e considerando uma necessária abordagem *Whole of Society* da

[12] O modelo conceptual procura fornecer os meios para abordar as vulnerabilidades, facilitar a deteção e fomentar a resiliência, adotando uma abordagem holística que considera devidamente a prevenção, preparação, resposta e recuperação. Também a NATO, aborda o CAH operacionalizado ao longo das três fases da sua estratégia: *Prepare – Detect – Deter*.

Defesa Nacional, para se definir quais as ações para prevenir e combater as AH, vamos valorizar os domínios do modelo conceptual como domínios de poder no CAH[13] e um ponto de referência para os decisores políticos, a fim de conceber políticas e ações eficazes e eficientes, especialmente quando se trata de deteção e de questões de atribuição destas ameaças de modo interministerial do Estado (*whole of government*) e holística multidisciplinar (*whole of society*).

Este modelo conceptual é ainda aberto, fornece um quadro flexível que permite a integração de novas ameaças e vulnerabilidades sem modificar significativamente os seus princípios fundamentais. (Giannopoulos & Smith, 2019), e que pode ser adaptado às necessidades de cada EM da UE e da NATO. Face a este pressuposto, nesta fase e, dispondo de capacidades neste âmbito, as vulnerabilidades nacionais e CAH assentam numa resposta articulada com a UE e a NATO. A maioria das ferramentas que podem visar o domínio espacial, explora a ligação do espaço com o ciberespaço e, com os outros domínios do CAH, realçando os potenciais efeitos em cascata, com forte ligação ainda, com o domínio militar, economia, infraestruturas, informacional e informações (Hybrid CoE, 2020), pelo que no caso nacional vamos associar este domínio ao domínio Ciber, pela exploração das suas capacidades.

Neste considerado, os domínios de poder do Estado para o CAH, nomeadamente da Defesa Nacional para apoiar a definição de estratégias nacionais são os: Político; Económico; Militar e Defesa; Diplomático; Informacional; Infraestruturas; Ciber e Espaço; Cultural; Administração Pública; Legal; Social; Informações.

4.3 Cooperação dos Domínios de Poder

Para a UE, esse esforço de cooperação é operacionalizado através da Criação da Célula de fusão da UE contra as AH para facilitar a partilha de conhecimento da situação, a fim de identificar qualquer alteração no contexto de segurança relacionada com uma atividade híbrida. Esta célula, ao apoiar a indicação das fontes e combater a desinformação concorre ainda em matéria de Comunicação Estratégica[14] dos EM. Através do Centro de Coordenação de Resposta de Emergência, a UE assegura a cooperação relativa à proteção

[13] Conjunto de capacidades que o Estado pode utilizar para elaborar as suas estratégias de CAH.
[14] Essencial para este efeito a ligação com o Centro de Excelência em Comunicações Estratégicas da NATO e Divisão STRATCOM da European External Action Service.

da saúde pública, para a qual concorrem as capacidades de proteção civil (Comissão Europeia, 2016a).

Para a NATO, a cooperação e coordenação da estratégia de CAH, são operacionalizadas ao longo de três fases: *Prepare – Detect – Deter*. Nas fases *Prepare* e *Detect* através dos mecanismos de recolha, tratamento e partilha da informação controlados pelo *Hybrid analysis branch*, que providencia aos decisores informação sobre as AH. A coordenação e cooperação são chave na medida em que a transnacionalidade da AH impele a um trabalho conjunto dos serviços de informação dos Estados, para que se possa antecipar acontecimentos em determinados países em face dos que ocorrem, no presente, noutros países. Também a formação e o treino conjunto / combinado melhoram a qualidade das respostas (militares e não militares), estimulando a cooperação e coordenação entre todos os domínios de poder e do setor privado. Na fase *Deter*, a cooperação e coordenação já estabelecida é central para o processo de tomada de decisão política e operacionalização dos instrumentos de resposta (NATO, 2019).

Em termos de visão, importa referir que, no contexto internacional, as estratégias, tanto da UE como da NATO, orbitam em torno da cooperação e coordenação para fazer face às AH. Esta assunção realça a constatação de que, a edificação desta capacidade, deve estar alicerçada numa resposta articulada com a UE e a NATO, sendo irrealista uma posição nacional singular na definição de uma estratégica nacional.

Sendo as AH passiveis de prosperar no anonimato, importa ainda a cooperação transversal interministerial e coordenação para aumentar a resiliência, garantindo maior capacidade nacional para recuperar a estabilidade, também face a vulnerabilidades identificadas.

Como referido no contributo do Ministério da Defesa Nacional (MDN) para a redação do documento de enquadramento nacional para fazer face às AH, apresentado ao MNE, em março de 2020, a resposta às AH só pode ser holística, abrangente, feita com todos e para todos.

Realça-se assim a necessidade de coordenação interministerial dos domínios das funções críticas da sociedade, tendente a para avaliação interna e ligação externa à NATO[15] e UE[16]. A coordenação e cooperação são assim elementos-chave na medida em

[15] Hybrid analysis branch.
[16] Célula de fusão contra as AH.

que a transnacionalidade da AH obriga a um trabalho conjunto de coordenação interministerial e dos serviços de informação dos Estados, para que se possa antecipar acontecimentos em face dos acontecimentos que ocorrem, no presente, noutros países.

Em 19 de Março de 2019, a UE adotou um regulamento[17]para criar um sistema de cooperação e troca de informações sobre investimentos de países não comunitários que possam afetar a segurança ou a ordem pública, tais como efeitos do investimento em infraestruturas e tecnologias críticas, fornecimento de inputs críticos (energia ou matérias-primas), acesso a informação sensível e capacidade de controlar a informação, ou a liberdade e pluralismo dos meios de comunicação social.

Perante este cenário, torna-se necessário apostar numa política de segurança interna e externa, cada vez mais assente numa maior colaboração e cooperação, integração e interdisciplinaridade interna e com a UE e os EM. Torna-se essencial redefinir o papel do Estado e reanalisar o conceito de Defesa Nacional, o Sistema de Segurança Interna (SSI) e, os modelos e sistemas de segurança e defesa.

O Estado Português tem como tarefas fundamentais, garantir a independência nacional e garantir os direitos e liberdades fundamentais e, promover o bem-estar e a qualidade de vida (art.º 9º da CRP).

As Forças de Segurança e as Forças Armadas (FFAA) assumem aqui um papel preponderante no âmbito da segurança do Estado, passando o seu conceito pela conjugação de áreas, consideradas "[…] estanques na dicotomia segurança interna/segurança externa e ao esforço coletivo na defesa" (Lopes, 2006, p. 10).

Pretende-se que a colaboração no âmbito do CAH, abranja a segurança e a defesa. Principalmente, pretendem-se políticas de segurança nacional, com uma maior cooperação e coordenação com políticas de segurança internacionais (NATO e UE), bem como uma gestão eficiente dos recursos humanos, das informações, das forças e serviços de segurança e de defesa, do poder judicial, do sector económico e financeiro, da tecnologia, da ciência e da diplomacia (Inácio, 2010).

O SSI dispõe de órgão principal, o Conselho Superior de Segurança Interna (CSSI)[18]. Fazem ainda parte do SSI, um Secretário-geral[19] e o Gabinete Coordenador de

[17] Regulation (UE) 2019/452 of the European Parliament and of the Council of 19 March 2019.
[18] Órgão de audição e consulta do Primeiro-ministro (art.º 13.º, n.º 1 e 2, alínea a) e b) da LSI).
[19] Com competências de coordenação, direção, controlo e comando operacional (art.º 14 a 19º da LSI).

Segurança[20]. O SSI, através dos seus três órgãos, detém assim mecanismos e competências para uma melhor interação com os outros sistemas internacionais da UE ou subsistemas nacionais, nomeadamente: o sistema de informações, a segurança aeronáutica e marítima, a segurança rodoviária e transportes, a segurança alimentar e económica e a segurança ambiental, o sistema criminal e a DN (Gabinete Coordenador de Segurança [GCS], 2008, p. 2).

Desde logo identificam-se necessidades de coordenação efetiva com os restantes domínios do CAH, nomeadamente Diplomático, Informacional; Ciber e Espaço; Cultura; Administração Pública; Legal; Social e o remanescente das Infraestruturas, bem como, no mesmo âmbito a efetiva coordenação no CAH com a UE e com a NATO.

No contexto nacional, aferimos a necessidade de um quadro legal de colaboração interministerial, e intersectorial (setor público e privado), que faça vigorar, a coberto de um documento nacional e respetivos planos operacionais a elaborar, medidas de coordenação e interoperabilidade de diferentes domínios de poder no âmbito da segurança nacional que não apenas o SSI[21] ou a DN. Embora não se enquadre no trabalho em curso, realçamos essa necessidade em face das observações evidenciadas por cinco entrevistados, questionados como visualizavam a centralidade da deteção, identificação, informação no âmbito da AH e, a colaboração interministerial, expressas no Quadro seguinte.

Quadro 3 – Registo de Observações à abordagem e coordenação interministerial

Entrevista	Observações
# 6	*"…, Lei de Segurança Interna (LSI) não responde às AH,…, rever a LSI alavancando o Conceito de Segurança Nacional (que não existe no conceito jurídico),…, potenciar o papel do SGSSI como elemento de comando e controlo da segurança nacional e na coordenação intergovernamental,…, possível replica nacional do* Hybrid Fusion Cell *e comités transversais nas diferentes áreas,…, identificar o SGSSI como interlocutor horizontal e de disseminação vertical com UE* Hybrid Fusion Cell *e NATO Hybrid Branch,…"*
# 8	*"…, não temos sistema de resiliência no âmbito da DN alargada onde se inclua a segurança nacional e que monitorize e identifique ameaças e riscos,…, deixou de haver Gabinetes de Crise para monitorização,…, o mecanismo de resiliência deve ser de cúpula em âmbito ministerial,…, acima de LSI e SGSSI englobando segurança e defesa,…, com Gabinete de Crise para as Ameaças"*
# 9	*"…, precisamos de uma Estratégia Global do Estado, com um Conceito Nacional de Segurança e Defesa, complementar e coordenada com a UE e NATO, e Visão a 10 anos,…, necessitamos de um Conceito de DN com abordagem por domínios,…, órgão*

[20] Órgão especializado de assessoria e consulta para a coordenação técnica e operacional da atividade das forças de segurança e funciona na direta dependência do Primeiro-ministro (art.º 21.º e 22.º da LSI).

[21] Realça-se o caso australiano, que para além de comité coordenadores de diferentes áreas do SSI e DN, dispõe também de comités coordenadores transversais de natureza jurisdicional, (National Security Science and Innovation Strategy, 2009, cap. 6).

	que faça levantamento de ameaças e análise,…, LSI não substitui um Conceito Estratégico de Segurança e Defesa,…, mais que uma revisão da LSI, para dar resposta à coordenação e complementaridade, precisamos de uma estratégia global e órgão que faça a articulação entre os diferentes pilares,…"
# 10	*"…, não temos sistema de análise de ameaças e riscos (Sistema de Resiliência Nacional),…, o critico para o CAH é a deteção, identificação e reporte,…, LSI, não responde às necessidades,…, não temos Conceito de Segurança e DN e não se visualiza revisão constitucional, pelo que necessitamos de uma estratégia global do estado,…, um Secretariado junto 1ºministro (órgão de conselho) para a segurança e defesa, com representação alargada e com um coordenador (National Security Advisor), este secretariado vai inclui e juntar vários outros comités como terrorismo e ciber.…, Sistema de Informações (SIRP) com responsabilidades alargadas e meios de pesquisa, análise e relato ao secretariado,…"*
#11	*"…, resposta às AH deve ser interdepartamental,…, Conceito de DN abrangente e compreensive,…, abordagem holística da DN, no âmbito multidisciplinar e global de segurança e defesa,…, Gabinete de crise de nível político para cooperação intergovernamental e para deteção, identificação e reporte de ameaças e riscos,…, na dependência do 1º ministro como responsável pela coordenação intergovernamental,…, se na dependência do MDN com uma abordagem compreensive da DN, implica alteração da constituição,..."*

Salienta-se a necessidade deste elemento de cooperação e coordenação interministerial para alimentar uma futura Estratégia Total no CAH, que promova a multidisciplinaridade dos domínios de poder, centralize a deteção, identificação, informação transversal e vertical com as estruturas da UE e NATO, das Ameaças e Riscos. Com base na informação recolhida e numa abordagem holística e multidisciplinar da Segurança e DN, visualiza-se um Gabinete ou Secretariado de Crise de nível político para cooperação intergovernamental e na dependência do Primeiro-Ministro como responsável pela coordenação intergovernamental. Órgão de conselho para a segurança e defesa, com representação alargada e com um coordenador, que seria responsável pela deteção, identificação e reporte de ameaças e riscos (incluindo assim vários outros comités atuais, como o do terrorismo e do ciber) e, orientando o esforço de pesquisa do Sistema de Informações (SIRP), como elemento central de pesquisa e relato. Este será um tema que se projeta para futuros desenvolvimentos, uma vez que não se constitui objeto deste trabalho.

4.4 Síntese Conclusiva

O atual espectro das ameaças para o Estado, nomeadamente a AH, obriga à mobilização de todos os recursos da nação, numa abordagem compreensiva e multidisciplinar da DN, englobando de modo holístico Segurança e Defesa, uma vez que para além da sua componente militar, a política de DN compreende as políticas sectoriais do Estado cujo contributo é necessário para a realização do seu interesse estratégico e para o cumprimento dos seus objetivos da DN.

As AH constituem, um desafio de natureza adaptativa, pelo que o seu combate inclui a sua prevenção, procurando preventivamente adquirir a consciência situacional e a resiliência nacional a esta ameaça, facilitando a sua deteção, a identificação e o combate, adotando um conceito que considere devidamente a prevenção, a preparação, a resposta e a recuperação. Nesta prevenção salienta-se a relevância da partilha de informação para um conhecimento situacional, sendo necessário a identificação dos elementos funcionais da rede de partilha, da rede de alerta e os elementos de combate; bem como o reforço da resiliência, nomeadamente a relativa à capacidade de garantir as funções vitais da sociedade numa situação de crise.

A análise dos documentos normativos estruturantes e a aplicação do contexto teórico de referência, permitiu a resposta à QD1 e o cumprimento do OE1, tendo identificado que os contributos da Defesa Nacional para o CAH, numa abordagem holística de Segurança e Defesa, concorrem com a utilização dos domínios de poder, Político, Económico, Militar e Defesa, Diplomático, Informacional, Infraestruturas, Ciber e Espaço, Cultural, Administração Pública, Legal, Social e, Informações, para o CAH e para a definição de estratégias nacionais e sectoriais.

Salienta-se ainda a necessidade de que, no contexto nacional, seja estudado um quadro de cooperação e coordenação interministerial, intersectorial e, entre setor público e privado e as organizações NATO e UE e, que se propõe, para futuros desenvolvimentos da temática da AH.

5. O ambiente externo face às Ameaças Híbridas

A análise do ambiente externo é relevante na definição de possíveis ameaças e riscos com as subsequentes oportunidades a alavancar. Ao ser, ainda, considerada a importância dos espaços cooperativos e colaborativos de que o país faz parte, assume-se relevante para Portugal a análise do quadro das AH enquanto membro da UE e da NATO, no âmbito dos espaços Político, Económico, Militar e Defesa, Diplomático, Informacional, Infraestruturas, Ciber e Espaço, Cultural, Administração Pública, Legal, Social e, Informações.

O ambiente internacional é de grande imprevisibilidade, com a prevalência de ameaças e riscos de tipo não convencional e caráter por vezes difuso e transnacional, expressos desde logo nas regiões confinantes do continente europeu: o Norte da África, o Médio Oriente, a Europa de Leste, a África Subsariana e Atlântico, nomeadamente no Golfo da Guiné (Despacho n.º 2536, 2020, p.2).

O modelo conceptual do Hybrid CoE, desenvolvido pela UE em dezembro de 2019[22], pretende apoiar os EM na definição de estratégias nacionais para a prevenção e combate das AH, sustentando-se nos atores, domínios e ferramentas e, visa identificar as ligações entre os estes, salientando-se a sua flexibilidade, que pode ser adaptado às necessidades de cada EM da UE e da NATO.

Importa, no caso nacional e tendo por base as ferramentas[23] da AH do modelo conceptual, expostas no Quadro 4 (desenvolvimento em Apêndice D), identificar, através das 17 entrevistas semiestruturadas a personalidades especialistas, as ameaças mais críticas e prováveis a Portugal, analisando também as possíveis oportunidades que se projetem em termos de ambiente externo, fruto do espaço geopolítico onde Portugal se integra.

Quadro 4 - Ferramentas do Combate de Ameaças Híbridas

Ferramenta
Operações físicas contra infraestruturas
Criar e explorar dependências em infraestruturas (incluindo dependência civil-militar)
Criar e explorar dependências económicas
Investimento direto estrangeiro
Espionagem industrial
Minar a economia nacional do adversário
Alavancagem de dificuldades económicas
Ciberespionagem

[22] Hybrid CoE (2020), *The Landscape of Hybrid Threats: A Conceptual Model*.
[23] Que combinadas, podem constituir AH.

Operações Ciber
Violação do Espaço Aéreo
Violação das Águas Territoriais
Proliferação de Armas
Operações militares convencional e não convencionais
Organizações Paramilitares
Exercícios Militares
Envolver as diásporas para influenciar
Financiamento de grupos culturais e de reflexão
Exploração de clivagens socioculturais (étnicas, religiosas e culturais)
Promover a agitação social
Manipular discursos sobre migração para polarizar as sociedades e minar as democracias liberais
Explorar as vulnerabilidades da Administração Publica (incluindo gestão de crises)
Promover e explorar a corrupção
Exploração de limites pouco claros, lacunas e ambiguidade da Lei
Alavancar argumentos, regras legais, processos, e instituições
Sistemas de Informações
Operações Clandestinas
Infiltração
Sansões Diplomáticas
Boicotes
Embaixadas
Criar confusão ou narrativas contraditórias
Migração como uma moeda de troca em relações internacionais
Desacreditação de lideranças e/ou candidatos
Apoio a atores políticos
Coerção de políticos e/ou governo
Exploração da imigração para influência política
Controlo e influência do Media
Campanhas de desinformação e propaganda
Influência curricular e académica
Operações eletrónicas (interferência de GNSS e falsificações)

Fonte: Hybrid CoE (2020)

5.1 Ambiente Externo - Quadro de Ameaças

A partir das respostas dadas à questão 1, elaboraram-se os quadros de análise das AH, com a respetiva análise categorial, desenvolvidos no Apêndice G. Da análise dos quadros, é possíveis concluir quais as ameaças mais críticas a Portugal e que serão as consideradas para o desenvolvimento das principais linhas de ação estratégicas no âmbito da Defesa Nacional para o CAH, expostas no Quadro 5.

Quadro 5 – Ameaças mais críticas num quadro de AH a Portugal

Ameaças Criticidade Alta	Domínio Base	Domínios Afetados
38. Campanhas de desinformação e propaganda	Social	Informacional, Político, Ciber, Cultural, Administração Publica
8. Ciberespionagem	Infraestruturas	Espaço, Ciber, Militar e Defesa, Administração Publica
9. Operações Ciber	Infraestruturas	Espaço, Ciber, Social, Administração Publica, Militar e Defesa
37. Controlo e influência do Media	Informacional	Infraestruturas, Social, Cultural
3. Criar e explorar dependências económicas	Economia	Diplomático, Político, Administração Publica
25. Sistemas de Informações	Informações	Militar e Defesa
5. Espionagem industrial	Economia	Infraestruturas, Ciber, Espaço, Informações, Informacional

26.	Operações Clandestinas	Informações	Militar e Defesa

Assim, de igual modo se pode inferir, que numa análise de domínio base (embora com uma afetação multidomínio), as ameaças mais críticas consideradas têm a seguinte distribuição expostas no quadro 6:

Quadro 6 – Domínios base das Ameaças mais críticas

Domínio Base	Ameaças
Social	Campanhas de desinformação e propaganda
Infraestruturas	Ciberespionagem e Operações Ciber
Informacional	Controlo e influência do Media
Economia	Criar e explorar dependências económicas e Espionagem industrial
Informações	Sistemas de Informações e Operações Clandestinas

5.2 Ambiente Externo - Quadro das Oportunidades

Decorrente das respostas dadas à questão 2 das entrevistas, elaboraram-se quadros de análise das AH com a respetiva análise categorial, desenvolvidos no Apêndice G. Da análise dos quadros do ambiente externo, referentes às oportunidades, é possível extrair o quadro de oportunidades consideradas mais relevantes e diretamente relacionadas com as ameaças mais críticas consideradas e respetivos domínios, expostos no Quadro 7.

Quadro 7 – Oportunidades do quadro de Ameaças críticas

Ameaça	Oportunidades
Campanhas de desinformação e propaganda	Gestão de perceções e educação social
	Comunicação estratégica
	Conhecimento situacional
	Estrutura de monitorização e identificação da ameaça e risco
Ciberespionagem e operações ciber	Estratégia de resiliência Ciber das Infraestruturas críticas
	Estrutura de monitorização e identificação da ameaça e risco
	Cooperação internacional NATO/UE
	Conhecimento situacional
Controlo e influência dos Media	Conhecimento situacional
	Estrutura de monitorização e identificação da ameaça e risco
Criar e explorar dependências económicas e espionagem industrial	Estratégia de resiliência económica em infraestruturas críticas
	Desenvolver indústria e planos de investimento
	Conhecimento situacional
Sistemas de Informações e Operações clandestinas	Cooperação internacional NATO/UE
	Estratégia de resiliência em ciberdefesa

5.3 Síntese Conclusiva

O ambiente internacional é de grande imprevisibilidade, com a prevalência de ameaças e riscos de tipo não convencional e caráter por vezes difuso e transnacional,

expressos desde logo nas regiões limítrofes do continente europeu. Assim a análise do ambiente externo é clara na definição de possíveis ameaças e riscos com as subsequentes oportunidades a alavancar, devendo ser considerada a importância dos espaços cooperativos e colaborativos de que o país faz parte, nomeadamente como membro da UE e da NATO.

Através da análise categorial, desenvolvida no Apêndice G, das 17 entrevistas semiestruturadas às entidades especialistas, foi possível identificar os quadros de ameaças mais críticas e prováveis a Portugal no âmbito do CAH e as oportunidades consideradas mais relevantes no contexto do espaço geopolítico onde Portugal se integra. Deste modo, identifica-se a necessidade de que, no contexto nacional, a análise da ameaça dever ser valorada enquanto membros da UE e NATO, e que a nossa resiliência à AH está diretamente ligada à coesão e unidade destas organizações.

Estamos assim em condições de responder à QD2, cumprindo o OE2, de analisar o ambiente externo face à AH e expor no Quadro 8, as principais ameaças e oportunidades face às AH.

Quadro 8 – Quadro de Ameaças e Oportunidades

Ameaça	Domínio Base	Domínios afetados	Oportunidades
Campanhas de desinformação e propaganda	Social	Social, Informacional, Político, Ciber, Cultural, Administração Publica	Gestão de perceções e educação social
			Comunicação estratégica
			Conhecimento situacional
			Estrutura de monitorização e identificação da ameaça e risco
Ciberespionagem e operações ciber	Infraestruturas	Infraestruturas, Espaço, Ciber, Militar e Defesa, Administração Publica, Social	Estratégia de resiliência Ciber das Infraestruturas críticas
			Estrutura de monitorização e identificação da ameaça e risco
			Cooperação internacional NATO/UE
			Conhecimento situacional
Controlo e influência dos Media	Informacional	Informacional, Infraestruturas, Social, Cultural	Conhecimento situacional
			Estrutura de monitorização e identificação da ameaça e risco
Criar e explorar dependências económicas e espionagem industrial	Económico	Económico, Diplomático, Político, Administração Publica Infraestruturas, Ciber, Espaço, Informações, Informacional	Estratégia de resiliência económica em infraestruturas críticas
			Desenvolver indústria e planos de investimento
			Conhecimento situacional
Sistemas de Informações e Operações clandestinas	Informações	Informações, Militar e Defesa	Cooperação internacional NATO/UE
			Estratégia de resiliência em ciberdefesa

6. O ambiente interno face às Ameaças Híbridas

Apesar dos progressos registados nas últimas décadas, persistem ainda algumas fragilidades nacionais que condicionam o desenvolvimento. Acresce, a estes desafios estruturais, a desaceleração económica causada pela pandemia, a qual tem tido um impacto significativo ao nível interno. No seu percurso, Portugal deverá atender ao desafio de promover a recuperação decorrente dos choques causados pela pandemia, potenciando a convergência com a UE, ao qual não será alheio o seu plano de recuperação e resiliência, para explorar as potencialidades e colmatar as vulnerabilidades internas.

A análise do ambiente interno, assenta nos treze (13) domínios do CAH, (em Apêndice C), para apoiar a conceção das ações certas a fim de enfrentar as AH. E conforme anteriormente referido, no presente trabalho vamos considerar doze (12) domínios, expressos no Quadro 9, para o CAH e, para a análise categorial no ambiente interno: Político; Económico; Militar e Defesa; Diplomático; Informacional; Infraestruturas; Ciber e Espaço; Cultural; Administração Pública; Legal; Social; Informações.

Quadro 9 – Domínios de poder

Domínios de poder para o CAH
Político
Económico
Militar e Defesa
Diplomático
Informacional
Infraestruturas
Ciber e Espaço
Cultural
Administração Pública
Legal
Social
Informações

Fonte: Comissão Europeia (2018)

Importa, no caso nacional e tendo por base os domínios expressos, identificar, através das 17 entrevistas semiestruturadas às entidades especialistas, as potencialidades e vulnerabilidades que se perspetivam a Portugal, analisando o ambiente interno.

6.1 Ambiente Interno – Quadro de Potencialidades

A partir das respostas dadas à questão 3, no 2.º bloco de questões, elaboraram-se os quadros de análise das potencialidades, com a respetiva análise categorial, desenvolvidos no Apêndice G. Da análise dos quadros, é possível concluir as potencialidades mais relevantes no ambiente interno num quadro de AH a Portugal e que no âmbito de trabalho

em apreço serão as que vão ser consideradas para o desenvolvimento das principais linhas de ação estratégicas no âmbito da Defesa Nacional para o CAH, expostas no Quadro 10.

Quadro 10 – Potencialidades por Domínio

Domínio	Potencialidades
Político	Sistema político consolidado e estável
	Posicionamento geopolítico e pertença à NATO e UE
Económico	Inovação e indústrias tecnológicas digitais e espaciais
	Espaço UE de trocas comerciais e progresso económico
Militar e Defesa	Dispersão territorial e prontidão
	Integração NATO, UE e participação missões ONU
Diplomático	Diplomacia consolidada
	Ligação CPLP e Lusofonia
Informacional	Pluralidade e confiança na informação
	Diversidade plataformas eletrónicas de comunicação
Infraestruturas	Planos Resiliência Infraestruturas
	Infraestruturas abastecimento espaço europeu
Ciber e Espaço	Cibersegurança
	Centros de inovação e polos tecnológicos
Cultural	Identidade e Unidade Cultural
	Sociedade plural e multicultural
Administração Pública	Modernização governativa e cidadania eletrónica
	Saúde, Justiça e Educação gratuitos
Legal	Separação poderes legislativo e judicial
	Proximidade dos cidadãos à justiça
Social	Unidade nacional e coesão social
	Garantia direitos fundamentais e proteção necessitados
Informações (Intel)	Sistema integrado de centralização Intel
	Intercambio Intel com NATO e UE

6.2 Ambiente Interno – Quadro de Vulnerabilidades

Decorrente das respostas dadas à questão 4 do 2.º bloco de entrevistas, elaboraram-se os quadros de análise das vulnerabilidades nacionais, com a respetiva análise categorial, desenvolvidos no Apêndice G. Da análise dos quadros do ambiente interno, é possível extrair o quadro de vulnerabilidades consideradas mais relevantes por domínios internos, expostos no Quadro 11.

Quadro 11 – Vulnerabilidades por Domínio

Domínio	Vulnerabilidades
Político	Falta consciencialização de ameaças e segurança
	Falta estratégia coordenação transversal e gestão crises integrada
Económico	Limitada competitividade económica e orçamental
	Dependência externa especialmente em recursos energéticos

Militar e Defesa	Falta de Investimento
	Resposta a ameaças multidominio e gestão crises
Diplomático	Pouca representatividade
	Falta Estratégia de cooperação e coordenação ameaças e riscos
Informacional	Consciencialização da ameaça
	Planos de ação e mecanismos de alerta
Infraestruturas	Falta Estratégia e planos de resiliência de infraestruturas
	Dependência Tecnológica
Ciber e Espaço	Estratégia espaço e resiliência ciber e digital
	Dependência tecnológica e dimensão económica
Cultural	Consciencialização da ameaça
	Capacidade económica
Administração Pública	Reforma digital e estrutural
	Falta de resiliência
Legal	Ferramentas legais pouco eficazes
	Sistema judicial moroso
Social	Literacia social
	Assimetrias sociais e demográficas
Informações (Intel)	Falta cultura e capacidades Intel
	Estratégia e resiliência Intel

6.3 Síntese Conclusiva

A nível interno, para além de desafios estruturais, a desaceleração económica causada pela pandemia, tem tido um impacto significativo. Portugal deverá atender ao desafio de promover a sua recuperação potenciando a convergência com a UE, ao qual não será alheio o seu plano de recuperação e resiliência, para explorar as potencialidades e colmatar as vulnerabilidades internas, de modo a preparar-se para a prevenção e CAH.

Através da análise categorial, desenvolvida no Apêndice G, das 17 entrevistas semiestruturadas às entidades especialistas, foi possível identificar os quadros de potencialidades mais relevantes e vulnerabilidades mais críticas no âmbito da prevenção e CAH, considerando os diferentes domínios do ambiente interno.

Estamos assim em condições de responder à QD3, cumprindo o OE3, de analisar o ambiente interno face à AH. Assim, como resposta à QD3, as principais potencialidades e vulnerabilidades no ambiente interno, são expostas no Quadro 12.

Quadro 12 – Quadro de Potencialidades e Vulnerabilidades

Domínio	Potencialidades	Vulnerabilidades
Político	Sistema político consolidado e estável	Falta consciencialização de ameaças e segurança
	Posicionamento geopolítico e pertença à NATO e UE	Falta estratégia coordenação transversal e gestão crises integrada
Económico	Inovação e indústrias tecnológicas digitais e espaciais	Limitada competitividade económica e orçamental

	Espaço UE de trocas comerciais e progresso económico	Dependência externa especialmente em recursos energéticos
Militar e Defesa	Dispersão territorial e prontidão	Falta de Investimento
	Integração NATO, UE e participação missões ONU	Resposta a ameaças multidominio e gestão crises
Diplomático	Diplomacia consolidada	Pouca representatividade
	Ligação CPLP e Lusofonia	Estratégia de cooperação e coordenação ameaças e riscos
Informacional	Pluralidade e confiança na informação	Consciencialização da ameaça
	Diversidade plataformas eletrónicas de comunicação	Planos de ação e mecanismos de alerta
Infraestruturas	Planos Resiliência Infraestruturas	Estratégia e planos de resiliência de infraestruturas
	Infraestruturas abastecimento espaço europeu	Dependência Tecnológica
Ciber e Espaço	Cibersegurança	Estratégia espaço e resiliência ciber e digital
	Centros de inovação e polos tecnológicos	Dependência tecnológica e dimensão económica
Cultural	Identidade e Unidade Cultural	Consciencialização da ameaça
	Sociedade plural e multicultural	Capacidade económica
Administração Pública	Modernização governativa e cidadania eletrónica	Reforma digital e estrutural
	Saúde, Justiça e Educação gratuitos	Falta de resiliência
Legal	Separação poderes legislativo e judicial	Ferramentas legais pouco eficazes
	Proximidade dos cidadãos à justiça	Sistema judicial moroso
Social	Unidade nacional e coesão social	Literacia social
	Garantia direitos fundamentais e proteção necessitados	Assimetrias sociais e demográficas
Informações (Intel)	Sistema integrado de centralização intel	Falta cultura e capacidades Intel
	Intercambio intel com NATO e UE	Estratégia e resiliência Intel

7. Análise de Strengths, Weaknesses, Opportunities e Threats (SWOT) e Linhas de Ação Estratégicas

Este subcapítulo tem como objetivo apresentar as principais linhas de ação estratégicas (LAE) para o CAH, deduzidas através da análise SWOT, correlacionando as potencialidades e vulnerabilidades, no ambiente interno, com as oportunidades e ameaças, do ambiente externo e a consequente confirmação por análise de validade.

A análise SWOT, tem por objetivo estabelecer prioridades de atuação e respetivas LA e baseia-se em quatro ideias chave: usar as potencialidades para obter vantagens sobre as oportunidades (PO); as oportunidades para superar as vulnerabilidades (VO); as potencialidades para evitar ameaças (PA); e em minimizar as vulnerabilidades para evitar ameaças (VA).

Para o efeito vão ser realizadas cinco análises SWOT, desenvolvidas em Apêndice H, numa análise para cada domínio base (embora com uma afetação multidomínio) das ameaças mais críticas identificadas, com uma posterior correlação final e identificação dos principais Objetivos Estratégicos nacionais no CAH e propor as respetivas LAE de acordo com as provas da estratégia pela validação por critérios de adequabilidade, aceitabilidade e exequibilidade.

7.1 Objetivos Estratégicos e Linhas de Ação no CAH

Das análises SWOT realizadas aos domínios Social, Infraestruturas, Informacional, Económico e Informações, apresentadas no Apêndice H e que se referem aos domínios base das ameaças mais críticas identificadas, identificam-se duas constatações. Identificam-se, desde logo, as principais linhas de ação (LA) no CAH que resultam das principais ameaças identificadas no âmbito do CAH e, simultaneamente assegura-se o seu enquadramento, agrupando as LA de acordo com as estratégias prioritárias identificadas nas dimensões do modelo de análise: (i) aumentar o conhecimento situacional; (ii) reforçar a resiliência; (iii) reforçar a capacidade de prevenir e dar resposta às crises e recuperar de forma coordenada na UE; (iv) reforçar a comunicação estratégica (Comissão Europeia, 2016b, 2018).

Nessa ótica, no Apêndice I, apresentam-se os objetivos e as 23 principais LA que resultam da análise SWOT e, as quais constituem um contributo e uma orientação para delineação de uma estratégia futura para o CAH.

7.2 Confirmação das linhas de ação estratégicas

Toda a estratégia tem a sua própria lógica inerente que deve ser confirmada para determinar a sua validade, deve promover a adequabilidade de recursos, a aceitabilidade de conceitos e a exequibilidade, pela satisfação das metas e interesses (Yarger, 2006, pg. 62).

Esta confirmação por validação de adequação, de exequibilidade e aceitabilidade, foi realizada com 4 entrevistas a entidades especialistas, que permitiram confirmar e consolidar as LAE no âmbito da Defesa Nacional para o CAH, em Apêndice I.

Assim, enquadrado nas provas da estratégia foi questionado, no âmbito da adequação, se a realização dos objetivos e LA propostas nos domínios indicados, vão produzir resultados; no âmbito da exequibilidade se as LA propostas, podem ser executadas com os recursos disponíveis; e no âmbito da aceitabilidade se os resultados esperados justificam as ações propostas nas LA.

As questões de adequação, exequibilidade, e aceitabilidade são questões para classificação de Elevada, Neutra ou Baixa incidem sobre a validade das propostas LA, pelo que é também questionado o risco, pela avaliação das prováveis consequências do sucesso e do fracasso das LA propostas, resultando num reescrever e melhoria das mesmas (Yarger, 2006, pg. 71).

7.3 Síntese Conclusiva

A dimensão multidimensional e transnacional das AH, vem reforçar a necessidade de existir uma visão alargada, com uma abordagem multi-instituicional, transversal e integrada *whole of government* e *whole of society* para se prevenir e combater a AH, aumentando a necessidade de reforçar a cooperação entre entidades no contexto nacional e no âmbito dos compromissos com as organizações de que faz parte (UE e NATO), através das sinergias da UE no âmbito da AH.

Através da análise SWOT, desenvolvida no Apêndice H, realizadas aos domínios Social, Infraestruturas, Informacional, Económico e Informações, foi possível identificar as 23 principais LA no CAH que resultam das principais ameaças identificadas no âmbito do CAH.

Posteriormente confirmaram-se as LA identificadas (Apêndice I), através de entrevistas de validação de adequação, exequibilidade, e aceitabilidade, pelo que estamos em condições de responder à QC, cumprindo o OG e propondo 21 LAE no âmbito da Defesa Nacional para o CAH, como resposta à QC, expostas no Quadro 13.

Quadro 13 – Objetivos e LA Estratégicas

ObjEst	LAE
Aumentar o Conhecimento Situacional	LAE 1 - Criar mecanismos de integração, de vigilância e alerta e coordenação interministerial de ameaças e riscos. LAE 2 - Reforçar a partilha de informação da situação das ameaças com NATO e UE e entre estas. LAE 3 - Promover a informação publica e educação da sociedade no âmbito das ameaças e dos riscos, nomeadamente na educação da cidadania e educação governamental.
Reforçar a Comunicação estratégica	LAE 4 - Promover a Comunicação Estratégica no domínio Social e Informacional, em coordenação com o CoE em Comunicação Estratégica da NATO e Divisão STRATCOM da EEAS. LAE 5 - Promover a capacidade de combate à desinformação, através de deteção precocemente e desmentidos rápidos e firmes
Reforçar a Resiliência	LAE 6 - Criar equipas de apoio e resposta a ameaça multidomínio para apoio a entidades e civis. LAE 7 - Criar mecanismos de certificação e validação em segurança ciber com apoio e coordenação com a UE. LAE 8 - Promover coordenação e integração entre as estratégias de resiliência ciber da UE, NATO e a Estratégia Nacional de Segurança do Ciberespaço. LAE 9 - Reforço do papel da inovação e do capital humano como fatores catalisadores da cibersegurança nacional. LAE 10 - Criar mecanismos legais de enquadramento do controlo da desinformação. LAE 11 - Promover mecanismos de dissuasão de ameaças híbridas através de ações punitivas em coordenação com UE e NATO. LAE 12 - Apoiar tecnologias disruptivas emergentes como IA e *big data* para detetar desinformação e vigilância Intel. LAE 13 – Promover e incrementar a captação de investimento e inovação em infraestruturas críticas. LAE 14 - Diversificar dependências energéticas através da promoção de parcerias e investimentos preventivos estratégicos e de mecanismos de cooperação europeus. LAE 15 - Incrementar estratégias de cooperação e parcerias económicas entre estado e privados. LAE 16 - Promover uma cultura e capacidade Intel nos diversos domínios de segurança nacional, reforçando mecanismos de cooperação civil-militar.
Reforçar a capacidade de prevenir e dar resposta a crises	LAE 17 - Elaborar plano de resiliência em infraestruturas critica com salvaguarda de cibersegurança e contraespionagem. LAE 18 - Elaborar plano de resiliência económico. LAE 19 - Elaborar plano de resiliência de Informações. LAE 20 - Elaborar plano de resiliência Informacional. LAE 21 – Planear e promover exercícios com elementos híbridos para treinar a resiliência.

8. Conclusões

O ambiente de segurança atual é cada vez mais complexo. Estão a acabar os tempos em que a paz, a crise e o conflito eram três fases distintas, em que os conflitos eram resolvidos fundamentalmente com meios militares, e os adversários eram conhecidos. Os ataques cibernéticos estão posicionados no espectro do conflito, abaixo do limiar de um ataque militar, as campanhas de media social e a exploração de dependências económicas criam alternativas que procuram desestabilizar países e entidades políticas sem emprego de meios militares. Acresce a combinação "híbrida" de instrumentos militares e não militares, que cria ambiguidades e que torna de elevada complexidade a consciência situacional e dificulta a rápida tomada de decisão.

O assunto passou a ser prioritário nas agendas da UE e da OTAN e o CAH assumiu também relevância na agenda nacional, visível na criação do grupo de trabalho para a elaboração do documento de enquadramento nacional das AH, bem como na relevância académica que o tema está a merecer, com vários seminários, artigos e estudos, e onde se insere também este TII.

O objeto do estudo deste trabalho foi a Defesa Nacional face às AH, propondo-se apresentar as principais LAE para o CAH numa abordagem *whole of government* e *whole of society*, no âmbito nacional e dos compromissos com as organizações de que faz parte, através das sinergias da UE no campo da AH.

Para a sua realização adotou-se uma investigação baseada num raciocínio indutivo, a metodologia seguiu a estratégia de investigação qualitativa e um desenho de estudo de caso, recorrendo à análise documental e a entrevistas semiestruturadas, como instrumentos de recolha de dados e, à análise de conteúdo e análise SWOT como técnicas de tratamento de dados.

A análise dos documentos normativos estruturantes e a aplicação do contexto teórico de referência, permitiu a resposta à QD1 e o cumprimento do OE1, tendo identificado que os contributos da DN para o CAH, numa abordagem multidisciplinar da DN englobando de modo holístico a Segurança e a Defesa, concorrem com a utilização dos domínios de poder, Político, Económico, Militar e Defesa, Diplomático, Informacional, Infraestruturas, Ciber e Espaço, Cultural, Administração Pública, Legal, Social e, Informações, para o CAH e para a definição de estratégias nacionais globais e sectoriais.

Através da análise categorial, às 17 entrevistas semiestruturadas a entidades especialistas, foi possível identificar os quadros de ameaças mais críticas e prováveis a Portugal no âmbito da prevenção e CAH e as oportunidades consideradas mais relevantes

no contexto do espaço geopolítico onde Portugal se integra, respondendo assim à QD2, e cumprindo o OE2, de analisar o ambiente externo face à AH. O tratamento da mesma análise categorial às entrevistas, permitiu ainda identificar os quadros de potencialidades mais relevantes e vulnerabilidades mais críticas no âmbito da prevenção e CAH, considerando os diferentes domínios do ambiente interno, respondendo à QD3, cumprindo o OE3, de analisar o ambiente interno face à AH.

Através da análise SWOT, realizada aos domínios Social, Infraestruturas, Informacional, Económico e Informações, foi possível identificar as 23 LA que resultam das principais ameaças identificadas no âmbito do CAH.

O processo de confirmação das LA identificadas, por entrevistas, realizou-se por validação de critérios de adequação, exequibilidade e aceitabilidade e, permitiu respondermos à QC, cumprindo o OG, de propor as LAE no âmbito da DN para o CAH.

Como principais resultados e contributos para o conhecimento, resulta a proposta de 21 LAE para apropriar o País no CAH, ao nível da DN, num conceito alargado de Segurança e Defesa e numa abordagem *whole of society*. Estas LAE, decorrem da identificação das ameaças consideradas mais prováveis e críticas e, da análise do ambiente externo e do ambiente interno, expressas na Figura 6.

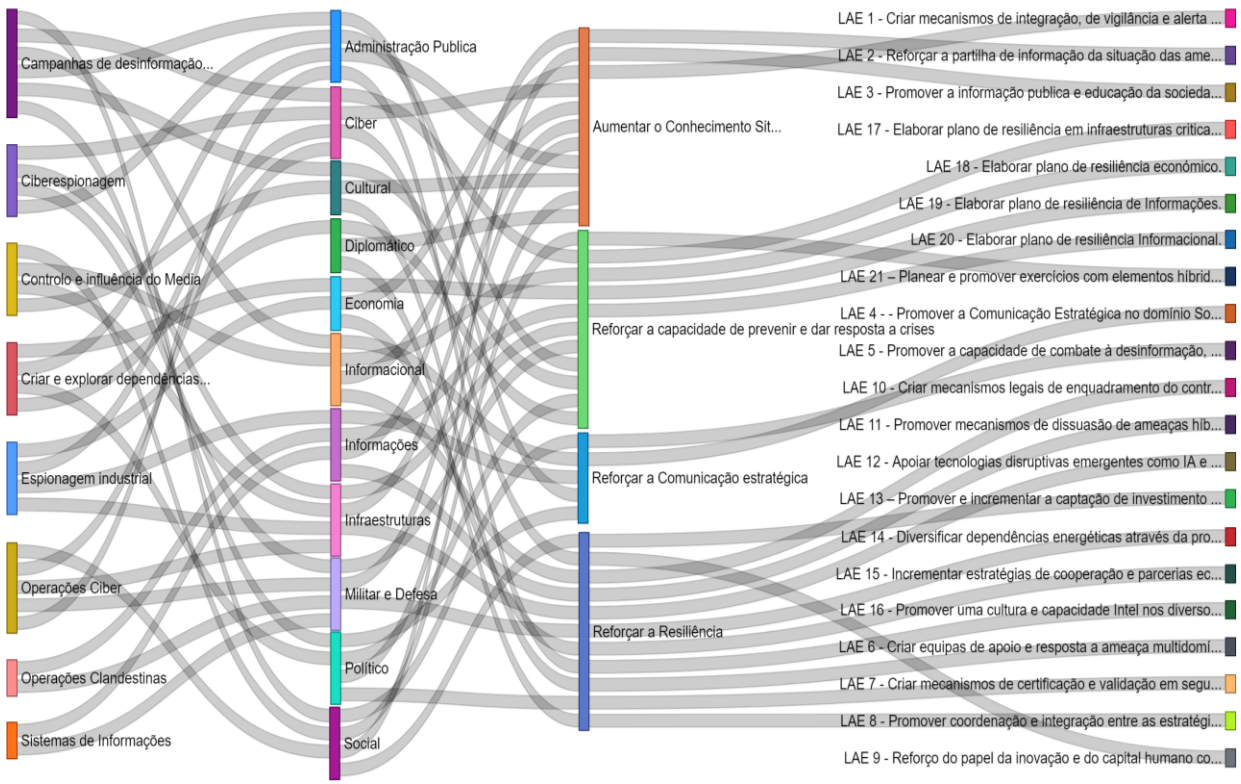

Figura 6 – Ameaças, Objetivos e Linhas de ação estratégicas no CAH

Em face dos Objetivos e LAE propõe-se a definição de uma estratégia nacional global para o CAH e a edificação das estratégias sectoriais no CAH para todos os domínios identificados, expressas na análise em *PowerBI* no apêndice I, realçando que na análise da ameaça dever ser valorada a nossa posição enquanto membros da UE e NATO e, que a resiliência nacional face à AH está diretamente associada à coesão e unidade destas organizações.

Como limitação à investigação, salienta-se a necessidade de uma análise nacional centrada em cada uma das possíveis ameaças e não apenas nas mais prováveis de modo a constituir-se verdadeiramente num documento de apoio a uma estratégia global.

Para proposta de investigação futura, identifica-se a necessidade de que, no contexto nacional, seja estudado um quadro de cooperação e coordenação interministerial, intersectorial e, entre setor público e privado e as organizações NATO e UE. Salienta-se a necessidade deste mecanismo de cooperação e coordenação para alimentar uma futura estratégia nacional no CAH, que promova a multidisciplinaridade dos domínios de poder, centralize a deteção, identificação, informação transversal e vertical com as estruturas da UE e NATO, centralizando a observação e coordenação das Ameaças e Riscos.

Referências Bibliográficas

Alves, M. (2020). *A prevenção e o combate às ameaças híbridas: impacto para as forças armadas portuguesas*. (Trabalho de Investigação Individual CPOG 2019/20). Lisboa: Instituto Universitário Militar.

Barroso, L. (2008, abril). Análise conceptual do Conceito Estratégico de Defesa Nacional. *Revista Militar*, 2475. Retirado de https://www.revistamilitar.pt/artigo/274

Bryman, A. (2012). *Social Research Methods (4ª ed.).* Oxford: Oxford University Press.

Coalson, R. (2016). The Value of Science Is in the foresight. *Military Review*, 23-29.

Comissão Europeia. (2016a). *Comunicação Conjunta ao Parlamento Europeu e ao Conselho. Quadro comum em matéria de luta contra as ameaças híbridas uma resposta da União Europeia*. Bruxelas: Comissão Europeia. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

Comissão Europeia. (2016b). Comunicado de imprensa- Segurança: *UE reforça resposta às ameaças híbridas*. Retirado de https://ec.europa.eu/commission/presscorner /detail/pt/

Comissão Europeia. (2018). *Increasing resilience and bolstering capabilities to address hybrid threats. Joint communication to the European Parliament, the European Council and the Council*. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018JC0016&from

Comissão Europeia. (2020). *Programa do Conselho para 18 meses (1 de julho de 2020 – 31 de dezembro de 2021)*. Secretariado-Geral do Conselho.

Couto, C. (1988*). Elementos de estratégia: apontamentos para um curso*. Vol. I. Pedrouços, Lisboa: Instituto de Altos Estudos Militares.

Declaração de Retificação n.º 52/2009, de 20 de julho, à Lei n.º 31-A/2009, de 7 de Julho (2009). *Rectifica a forma e o número da Lei n.º 31-A/2009, de 7 de Julho, publicada no Diário da República, 1.ª Série, n.º 129 (suplemento), de 7 de Julho de 2009, que se rectifica como Lei Orgânica n.º 1-B/2009, de 7 de Julho, e republicação integral da mesma*. Diário da República, 1ª Série, 138. Lisboa: Assembleia da República.

Decreto-Lei n.º 249/2015, de 28 de outubro (2015). *Aprova a orgânica do ensino superior militar, consagrando as suas especificidades no contexto do ensino superior, e aprova o Estatuto do Instituto Universitário Militar*. Diário da República, 1.ª Série, 211, 9298-9311. Lisboa: Ministério da Defesa Nacional.

Despacho n.º 7769/2010, de 4 de maio (2010). Determina a publicação da Directiva Ministerial de Defesa 2010-2013. Diário da República, 2.ª Série, 86. Lisboa: Gabinete do Ministro da Defesa Nacional.

Despacho n.º 2536/2020, de 24 de fevereiro. (2020). *Diretiva Ministerial de Planeamento de Defesa Militar - quadriénio 2019-2022*. Diário da República, 2.ª Série, 38, 36-41. Lisboa: Ministério da Defesa Nacional.

Dias, A. L., Varela, M., & Costa, J. L. (2013). *Excelência Organizacional*. Lisboa: Editora Bnomics.

Diretiva n.º 114/2008/CE do Conselho, de 8 de dezembro (2008). *Relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção*. Jornal Oficial da União Europeia. Retirado de http://data.europa.eu/eli/dir/2008/114/oj

European External Action Service. (2015). C*ountering Hybrid Threats, Food-for-thought paper. Information & Security*. Retirado de http://isij.eu/article/countering-hybrid-threats-food-thought-paper

Fachada, C. P. A., Ranhola, N. M. B., Marreiros, J. P. R., & Santos, L. A. B. (2020). *Normas de Autor no IUM* (3.ª Ed., revista e atualizada). IUM Atualidade, 7. Lisboa: Instituto Universitário Militar.

Fernandes. (2016). As Novas Guerras: O Desafio da Guerra Híbrida. *Revista de Ciências Militares*, p. 20.

Fleming, B. (2011). *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art.* School of Advanced Military Studies.

Freedman, L. (2015). *Strategy*. Oxford University Press: US.

Gabinete Coordenador de Segurança. (2008). *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna.

Giannopoulos, G., & Smith, H. (2019). *The Landscape of Hybrid Threats: A conceptual model*. Brussels: European Commission.

Guindo, M. (2015). *La guerra híbrida: Nociones preliminares y su repercusión en el planeamiento de los países y organizaciones occidentales*. Instituto Español de Estudios Estratégicos (IEEE), p. 3.

Hybrid CoE. (2017). *Hybrid Threats*. The European Centre of Excellence for Countering Hybrid Threats: https://www.hybridcoe.fi/hybrid-threats/

Hybrid CoE. (2019). *Countering Hybrid Threats - Understanding Hybrid Warfare*. Retirado de https://www.hybridcoe.fi/hybrid-threats/

Hybrid CoE. (2020). *The Landscape of Hybrid Threats: A conceptual model*. Brussels: European Commission.

Hoffman, F. (2007). C*onflict in the 21st Century: The rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies, p.14.

Inácio, C. (2010). *Políticas Públicas de Segurança – novo paradigma* (Dissertação de Mestrado em Ciência Política). Secção Autónoma de Ciências Sociais, Jurídicas e Políticas, Universidade de Aveiro.

Lei n.º 53/2008, de 29 de agosto (2008). *Aprova a Lei de Segurança Interna*. Diário da República, 1.ª Série, 167. Lisboa: Assembleia da República.

Lopes, A. (2006). Segurança e Cidadania: conceitos e políticas. Grupo de estudo e reflexão de estratégia. *Cadernos Navais*, 19. Edições culturais da marinha. Out/Dez.

Lopes. (2017). *O Terrorismo Transnacional e as Novas Guerras*. *Impactos para as Forças Armadas Portuguesas*.

LUSA. (2019). *Candidatura ao Centro Europeu de Excelência para Combate às Ameaças Híbridas*. Retirado de https://combatefakenews.lusa.pt/fake-news-governo-quer-plano-nacional-para-combater-desinformacao-e-ciberataques-c-audio/

Markopouloua, V. (2019). *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law and Security Review*.

Milinko, & Ćurčić (2018). T*he evolution of European Perception of the term "Hybrid Warfare*". Belgrado: VOJNO DELO.

Ministério da Defesa Nacional. (2014). *Conceito Estratégico Militar – CEM 2014. Aprovado pelo Ministro da Defesa Nacional em 22 de julho de 2014. Confirmado em Conselho Superior de Defesa Nacional de 30 de julho de 2014*. Lisboa: Ministério da Defesa Nacional.

Monaghan. (2019). *Countering Hybrid Warfare: Concetual Foundations and Implications for Defence Forces - Information note. MCDC Countering Hybrid Warfare Project*.

Multinational Capability Development Campaign. (2017). Countering Hybrid Warfare Project: Understanding Hybrid Warfare. *MCDC January 2017.*

Multinational Capability Development Campaign. (2019). *Countering Hybrid Warfare Information Note.* Gov.UK Ministry of Defence. Retirado de

https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare

Myklín. (2018). *Russian Non-Linear Warfare Through the Lenses of Strategic Culture*. Brno: Universidade de Masaryk.

National Security Science and Innovation Strategy. (2009). *The National Security Science and Innovation Strategy*. Australian Government.

NEP/INV-001 (A1). (2020a, setembro). *Procedimentos relativos à elaboração de trabalhos de investigação realizados no âmbito de cursos que não atribuem grau académico*. Lisboa: Instituto Universitário Militar.

NEP/INV-003 (A3). (2020b, setembro). *Estrutura e regras de citação e referênciação de trabalhos escritos a realizar no Instituto Universitário Militar*. Lisboa: Instituto Universitário Militar.

North Atlantic Treaty Organization. (2010, agosto). *Bi-SC Input to a New NATO Capstone Concept for a Military contribution to Countering Hybrid Threats*. Retirado de https://www.act.nato.int/images/stories/ events/2010/20100826_bi-sc_cht.pdf

North Atlantic Treaty Organization. (2013). *Allied Command Operations Comprehensive Operations Planning Directive Interim V2.0*. Belgium: North Atlantic Treaty Organization, Supreme Headquarters Allied Powers Europe.

North Atlantic Treaty Organization. (2014). *Wales Summit Declaration, Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*. Retirado de https://www.nato.int /cps/en/natohq/official_texts_112964.htm

North Atlantic Treaty Organization. (2015). *Hybrid Warfare: NATO's New Strategic Challenge*.

North Atlantic Treaty Organization. (2018). *Brussels Summit Declaration, Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels July 2018*. Retirado de https://www.nato.int/cps/en/natohq/official_texts_156624.htm

North Atlantic Treaty Organization. (2019). NATO. Retirado de www.nato.int: https://www.nato.int/cps/en/natohq/topics_156338

North Atlantic Treaty Organization. (2020). *Resilience and Article 3*. Retirado de *https://www.nato.int/cps/en/natohq/ topics_ 132722.htm*

North Atlantic Treaty Organization. (2017). *Allied Joint Doctrine Edition E Version 1*. AJP-1. NATO Standardization Office (NSO). NATO.

Nye Jr, J. (2008). *The Powers to Lead.* Oxford University.

Pereira. (2018). *As ameaças híbridas - Uma abordagem conceptual no quadro da OTAN e da UE*. CEDIS.

Puyvelde. (2015). Hybrid war – does it even exist? *NATO Review*. Retirado de https://www.nato.int/ docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html

Ralph. (2016). *Hybrid Warfare - On redisign of National Security*. ISPS Strategics studies.

Ramalho, P. (2005). O conflito assimétrico e o desafio da resposta - Uma reflexão. *Revista Militar* 2443/2444 ago/set.

Rego, A., Cunha, M. P., & Meyer, Victor. (2019). Quantos participantes são necessários para um estudo qualitativo? Linhas práticas de orientação. *Revista de Gestão dos Países de Língua Portuguesa*, 45-57. Retirado de https://doi.org/ 10.12660/rgplp.v17n2.2018.78224.html

Resolução do Conselho de Ministros n.º 19/2013, de 21 de março (2013). *Aprova o Conceito Estratégico de Defesa Nacional*. Diário da República 1.ª Série, 67, 1981-1995. Lisboa: Presidência do Conselho de Ministros.

Santos & Lima. (2019). *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação* (2.ª ed, revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Sarmento, M. (2013). *Metodologia Científica para a elaboração, escrita e apresentação de teses*. Lisboa: Universidade Lusíada.

Serrão, D. (2019). *Visita ao Centro Europeu de Excelência para o combate às ameaças híbridas*. Lisboa: IUM.

Steder. (2016). *The Theory, Históry, and Current State of Hybrid Warfare*. Oslo: Norwegian Defence Research Establishment.

Treverton. (2018). *Addressing Hybrid Threats.* Swedish Defence University.

U.S. GAO. (2010). *U.S. Government Accountability Office*. Retirado de : http://www.gao.gov/assets/ 100/97053.pdf

Yarger, H. (2006). *Strategic Theory for the 21st Century: The Little Book on Big Strategy, Carlisle: Strategic Studies Institute*. USAWC.

Apêndice A — Corpo de conceitos

Ameaça	Qualquer acontecimento ou ação – em curso ou previsível –, de variada natureza – militar, económica, ambiental, etc. – que contraria a consecução de um objetivo e que, normalmente, é causador de danos, materiais ou morais, sendo que no âmbito da estratégia consideram-se principalmente as ameaças provenientes de uma vontade consciente, analisando o produto das possibilidades pelas intenções" (Couto, 1988).
Ameaças	São os imprevistos ou potenciais problemas que podem ser considerados como fatores de risco, desafios que já são reconhecidos ou que surgem como obstáculos novos. Em outras palavras, aspetos externos que representam riscos para a organização (Dias et al., 2013).
Ameaça Híbrida	Ações coordenadas e sincronizadas que visam deliberadamente afetar as vulnerabilidades dos Estados democráticos e das suas instituições, empregando um leque particularmente amplo de meios políticos, económicos, militares, civis e de informação (Hybrid CoE, 2019).
Ator não-estatal	O Estado não é o único ator, na atualidade verifica-se que surgem diversas unidades coletivas de dimensão variável, internas e externas, com ou sem base territorial, que se constituem como entidades políticas, afirmando a sua identidade, a sua autoridade e a sua autonomia de decisão no seio da sociedade internacional. Estas entidades realizam ações de natureza estratégica em virtude de os seus projetos políticos interagirem com os de outras entidades, gerando situações litigiosas (Ribeiro, 1999).
Centro de Gravidade	É a fonte de poder que fornece força moral ou física, liberdade de ação, ou vontade de agir, a um sistema, ator estatal ou não-estatal (Couto, 1988).
Espaço Estratégico de Interesse Nacional Permanente	Espaço Estratégico de Interesse Nacional Permanente é o espaço que corresponde ao território nacional compreendido entre o ponto mais a norte, no concelho de Melgaço, até ao ponto mais a sul, nas ilhas Selvagens, e do seu ponto mais a oeste, na ilha das Flores, até ao ponto mais a leste, no concelho de Miranda do Douro, bem como o espaço interterritorial e os espaços aéreos e marítimos sob responsabilidade ou soberania nacional. (Ministério da Defesa Nacional , 2014).
Funções críticas	São funções ou sistemas distribuídos no espectro político, militar, económico, social, informacional e infraestruturas (PMESII); cuja descontinuação pode levar à interrupção dos serviços dos quais um sistema operacional depende. As funções críticas podem ser divididas em indivíduos ou organizações, infraestruturas (e.g. redes de energia nacionais críticas) e processos (e.g. legais, jurisdicionais, técnicos, políticos) (MCDC, 2019).
Guerra Híbrida	Consiste no desafio apresentado pela crescente complexidade do conflito armado, em que os adversários podem combinar diferentes tipos de guerra com meios não militares para neutralizar o poder militar convencional (MCDC, 2019).
Hard Power	É quando se emprega a coação, seja através do emprego da força militar ou económica (Nye Jr, 2008).
Instrumentos de Poder	Das fontes de Poder emanam um conjunto de capacidades que o Estado pode utilizar para elaborar as suas estratégias e podem ser sistematizados, assumindo a designação de instrumentos do Poder (AJP-01, 2017).
Oportunidades	São os caminhos ou espaço para crescimento, que podem ser desenvolvidos para suprir necessidades. Em outras palavras, são aspetos externos positivos, que quando utilizado em conjunto com o que a organização tem de positivo internamente, podem ser transformados em oportunidades de melhoria (Dias, Varela, & Costa, 2013).
Potencialidades	São os pontos positivos, aspetos em que a organização se destaca internamente e que constituem uma vantagem face a outras organizações (Dias et al., 2013).
Resiliência	Capacidade que a sociedade tem para resistir e recuperar com facilidade de choques que causem grande impacto, como é o caso de calamidades, falhas de infraestruturas críticas ou ataques armados, utilizando a sua *civil preparedness* e a sua capacidade militar (NATO, 2020).
Smart power	É a combinação de hard *power* com o soft *power*, onde não se descarta o uso da força militar quando necessário para que os objetivos sejam alcançados (Nye Jr, 2008).
Soft Power	É a capacidade de um ator das relações internacionais obter o que deseja através do poder da atração e não da coação (Nye Jr, 2008).
Vulnerabilidades	São os pontos negativos, desvantagens da organização em relação a concorrentes, principais erros já cometidos, o que já foi reconhecido com um problema ou erro (Dias et al., 2013).

Apêndice B — Antecedentes de Guerra e Ameaça Híbrida

1. Antecedentes

Em 2002, o Major dos *United States Marine Corps*, William Nemeth, utiliza o termo de GH para refletir no modo de contrariar as ações das sociedades híbridas e mistas, investigando o caso do conflito da Tchetchénia. Definiu GH como a guerrilha contemporânea que utiliza coordenadamente a tecnologia moderna e que explora as relações entre entidades civis e militares, bem como a combinação das ações resultantes de abordagens tracionais, com abordagens mais modernas e complexas (Steder, 2016).

O conceito de GH vem responder à necessidade de compreender a nova fisionomia da guerra e os problemas práticos vividos pelas FFAA Americanas que se vêm mostrando ineficientes nos conflitos assimétricos[24] em que participam (Milinko & Ćurčić, 2018).

Apesar de conceito novo, muitos teorizadores referem que estas estratégias híbridas já são utilizadas há muito tempo. A história está repleta de exemplos de estratégias híbridas, nomeadamente na Revolução Americana (1775-83), com a participação e envolvimento de milícias e, nas invasões napoleónicas, com as forças regulares britânicas a cooperar com guerrilhas (Hoffman, 2007). Mais recentemente, na II Guerra Mundial, alguns aspetos da GH também foram explorados, nomeadamente a disseminação de informações falsas no inimigo e o uso combinado de forças irregulares com o esforço diplomático para tentar atrair aliados e isolar adversários. No século XXI atores como o Hezbollah, a Al Qaeda e, a Rússia no conflito da Ucrânia, vêm revelar-se como principais protagonistas da GH (Treverton, 2018).

Importa ainda salientar, a influência dos coronéis chineses Qiao Liang e Wang Xiangsui, que procuraram expandir a definição e compreensão da guerra além do campo militar tradicional, naquilo que chamaram a guerra sem restrições ou além dos limites, para enfrentar as vantagens dos estados com mais poderio militar e tecnológico (Guindo, 2015).

A primeira vez que o conceito de GH aparece no vocabulário militar e ganha conteúdo, foi em 2005 com o artigo de Mattis e Hoffman[25] "*Future Warfare: The Rise of Hybrid Wars",* publicado na prestigiada revista *Proceedings*. Nele, os autores alertam para o facto, de que a superioridade dos Estados Unidos estava a levar os restantes atores estatais e não estatais a abandonarem a maneira tradicional de fazer a guerra, procurando outros tipos com a combinação de tecnologias e táticas para obter vantagens (Guindo, 2015).

Posteriormente, Hoffman em 2007, vem consolidar o conceito, sustentando que, para além de uma evolução no modo de conduzir a guerra, vivemos numa época em que diversos tipos de guerra são conduzidos simultaneamente por adversários ágeis, flexíveis e sofisticados que têm a visão da multiplicidade de meios e efeitos para mais facilmente contribuírem para atingir os objetivos. No desenvolvimento das teorias da GH, observa que é demasiado simplista classificar meramente os conflitos como grandes e convencionais ou pequenos e irregulares, já que a tendência será para o emprego combinado de diferentes tipos de guerra. Define que as AH conjugam diferentes modos de fazer a guerra, incluindo capacidades convencionais e táticas irregulares, atos terroristas incluindo violência e coesão indiscriminada e criminalidade, podendo as guerras híbridas ser conduzidas por estados e atores não estatais (Hoffman, 2007). Originalmente, a atribuição da classificação de GH, foi feita ao Hezbollah em 2006, na segunda guerra do Líbano, por ter usado guerra convencional, não convencional, regular e irregular, aberta e encoberta e, ter explorado todas as dimensões para combater a superioridade convencional do adversário (Puyvelde, 2015).

Em síntese e, antes da intervenção da Rússia na Crimeia, GH e AH, tinham já entrado no léxico dos investigadores e decisores, evidenciando elementos caracterizadores, nas dimensões *Ends, Ways* e *Means*, nomeadamente dirigidas e coordenadas no mesmo espaço de batalha para alcançar efeitos sinérgicos nas dimensões físicas e psicológicas do conflito; utilização coordenada de tecnologia com métodos de mobilização; combinação de capacidades disruptivas com formas tradicionais, irregulares e; estímulo da globalização, modos combinados de conduzir a guerra convencional e irregular; atores não-estatais usando de tecnologias sofisticadas e, adversários ágeis e flexíveis que têm a visão da multiplicidade de meios e efeitos nos diferentes domínios para atingir os objetivos.

No seu artigo de 2013, o General Valery Gerasimov, "*The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*", publicado no jornal de negócios semanal russo *Military-Industrial Kurier*, faz uma comparação de meios entre a forma

[24] Ações conduzidas por atores ou estados, com vista a ultrapassar ou negar capacidades do oponente, pondo ênfase na afetação/agravamento das vulnerabilidades percebidas; utiliza meios não habituais, que ponham em causa valores distintos ou antagónicos, levando a cabo estratégias não tradicionais, empregando capacidades não convencionais ou não ortodoxas, para atingir os seus fins (Ramalho, 2005).

[25] A 8 de setembro de 2005, no Fórum de Defesa do Instituto Naval e Associação do Corpo de Marines.

tradicional de conduzir a guerra, com uso exclusivo de forças militares e, a nova forma de fazer a guerra com o uso de meios políticos, diplomáticos, económicos e a combinação de medidas não militares com o uso de forças militares (Coalson, 2016). A aplicação desse pensamento estratégico sentiu-se no posicionamento da Rússia na intervenção militar no leste da Ucrânia e anexação da Crimeia, em que aproveitou focos de uma crise persistente para, exponenciando-os, reanexar parte do território de um país legítimo e soberano[26].

Apesar do termo "hybrid" ganhar dimensão na doutrina americana, nomeadamente para descrever o aumento da complexidade dos conflitos atuais, oficialmente não é considerado uma nova forma de guerra. No relatório "*Government Accountability Office* (GAO)", de setembro de 2010, os EUA não adotaram o termo "guerras híbridas", por considerarem que está abrangido pelas *full spectrum operations*, não fazendo referências explicitas nas suas últimas estratégias nacionais de segurança (US GAO, 2010).

No entanto, a UE e a NATO mostraram uma abordagem diferente. A UE, através de um documento do "*European External Action Service (Countering hybrid threats, food-for-though paper*)", caraterizou a GH como o uso centralmente concebido e controlado de várias táticas encobertas e abertas, decretadas por meios militares e não-militares, que vão desde operações de informações e cibernéticas através de pressão económica para o uso de forças convencionais (European External Action Service [EEAS], 2015).

Por sua vez a NATO, define GH como o uso de táticas assimétricas para investigar e explorar fraquezas por meios não militares (como intimidação e manipulação política, informativa e econômica), os quais são apoiados pela ameaça de meios militares convencionais e não convencionais. (NATO, 2015).

No mesmo alinhamento de combinar ações recorrendo a diferentes meios, a Universidade da Defesa da Suécia[27], identifica 16 ferramentas, com grande enfase no domínio informacional, nomeadamente através da Propaganda; Uso dos Media, Media Sociais e *fake news*. Salienta que a GH é, essencialmente, assimétrica, atuando nos diferentes instrumentos de poder: verticalmente intensificando efeitos com uso de uma ou mais ferramentas e horizontalmente combinando os efeitos gerados, exponenciando-os (Treverton, 2018).

O conceito de GH caracteriza-se, por ações combinadas, sincronizadas e executadas de forma sequencial, com recurso a diversos instrumentos de poder para alcançar objetivos políticos e estratégicos. Ao contrário do conceito de *Military Centric Warfare*, em que a guerra se baseia sobretudo no domínio militar, a condução de uma GH passa por coordenar ações nos diversos domínios (Serrão, 2019).

Segundo Schmid, a GH difere das conceções clássicas da guerra em três aspetos: i) no foco da decisão; ii) na condução das operações; iii) no emprego de meios e métodos. O foco da decisão incide nos centros de gravidade (CoG) não militares que são mutáveis ao longo do tempo, criando ambiguidade e impedido a compreensão da situação e os domínios explorados pelas ações cobrem todo o espectro (Schmid, 2019). As operações são conduzidas numa "*Grey Zone*", face à complexidade de identificação dos seus elementos e fronteiras. A plasticidade da GH compreende múltiplos interfaces, posicionando-a desde a paz à guerra e, caracterizando-se pelo contacto direto como amigo, população e inimigo, através da criação de contextos de aparente apoio externo para legitimar ações que se destinam, a corroer, a segurança interna e a expor vulnerabilidades do país (Schmid, 2019). A GH é uma amálgama de *softpower* com *hardpower*, catalisado com a criatividade característica do *smartpower* (Hybrid CoE, 2020).

Quanto à utilização de meios e métodos, a GH caracteriza-se pelo uso combinado de meios civis e militares, regulares e irregulares, usados de forma aberta e coberta. A GH visa criar uma atmosfera de confusão generalizada para expor vulnerabilidades, onde esta amálgama de ações e efeitos, confunde a identificação clara de padrões, racionais e, por vezes, até do responsável pelas ações. Assim, o domínio militar assume-se como um elemento de suporte e as vitórias são, em larga medida conseguidas, atingindo-se e explorando os CoG não militares (Freedman, 2015).

2. Ameaças Híbridas

O conceito de AH tem sofrido uma evolução ao longo dos últimos anos, sendo complexo distinguir claramente AH de GH (MCDC, 2019). O conceito de AH surge em 2008, sendo definido pelo então Chefe do Estado-Maior do Exército americano como, "um adversário que incorpora combinações diversas e dinâmicas de capacidades convencionais irregulares, terroristas e criminosas" (Fleming, 2011), aparecendo posteriormente em 2010, em documentos oficiais da NATO, definida como, "*Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means*

[26] Explorando as fragilidades resultantes de fracionamentos históricos, culturais e sociais na Crimeia, a Rússia fez uso de *proxies* e grupos como "*Night Wolves*" para ações de desestabilização, projetaram militares descaracterizados para ações de reconhecimento e vigilância "*little green men*", desenvolveram ataques "Ciber" inviabilizando redes móveis, associada a uma campanha de desinformação (Myklín,2018).

[27] Treverton. (2018). *Addressing Hybrid Threats,* com o apoio do *Center for Assymetric Threat Studies* e do Hybrid CoE.

adaptively in pursuit of their objectives" (NATO, 2010, p. 2). Em 2016 a UE define as AH como "*a mixture of coercive and subversive activity, conventional and unconventional methods,* […] *which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of open organized hostilities*" (Comissão Europeia, 2016a, p. 4). A evolução conceptual[28], acomodou as novas tendências tecnológicas, verificando-se atualmente o seu uso generalizado nos documentos e na estratégia de segurança euro-atlântica. Apesar das possíveis divergências, a maioria dos conceitos assenta na abordagem do teorizador da Arte da Guerra, Sun Tzu, a de uma estratégia não violenta na política internacional e, pelo uso de múltiplos meios para atingir vulnerabilidades em toda a sociedade, para alcançar objetivos, sem desencadear respostas decisivas ou armadas (MCDC, 2019).

O Hybrid CoE (2019), entende a AH como ações coordenadas e sincronizadas que visam deliberadamente afetar as vulnerabilidades dos Estados democráticos e das suas instituições, empregando um leque particularmente amplo de meios políticos, económicos, militares, civis e de informação. Este centro de excelência apresenta como principais características das AH: i) a ação coordenada e sincronizada, que visa deliberadamente vulnerabilidades sistémicas dos estados e instituições democráticas, através do emprego de uma ampla gama de meios; ii) essas atividades exploram os limites de deteção e da legalidade, os interfaces da paz e guerra, interno-externo, local-estado, nacional-internacional, amigo- inimigo; iii) o objetivo da atividade é influenciar a tomada de decisão ao nível local, estatal ou institucional. (Hybrid CoE, 2019).

3. Linhas de ação da NATO para o Combate de Ameaças Híbridas

Verificou-se pela primeira vez na Cimeira de Lisboa[29] uma preocupação com as AH, afirmando-se o empenho da Organização em deter, defender-se contra qualquer ameaça de agressão e se preparar para os desafios emergentes à segurança, dos Aliados, individualmente ou da Aliança como um todo (NATO, 2010). Os futuros desafios englobam atores estatais ou não estatais, que usam sistematicamente e de modo adaptável, formas e métodos combinados para alcançar os seus objetivos políticos.

Na Cimeira de 2014[30,] em Gales, é oficialmente afirmada a condição de que a NATO deve ser capaz de lidar com os desafios das AH, considerando a posse de ferramentas e procedimentos para dissuadir e responder fundamentais, como o desenvolvimento da comunicação estratégica, de cenários com AH e o fortalecimento da coordenação, cooperação e complementaridade entre a NATO e outras organizações (NATO, 2014). O aprofundamento do tema da AH, entre 2014 e 2016 ficou espelhado na centralidade ocupada na Cimeira de Varsóvia[31], sublinhando-se a necessidade de uma estratégia NATO em coordenação com a UE para "Countering Hybrid Warfare". Aponta a responsabilidade primária de resposta aos países membros e a capacidade de os apoiar em qualquer que seja a fase da campanha híbrida à Organização (NATO, 2018). Em linha com a dupla ideia dos novos desafios pressionarem primeiramente os frágeis e que países resilientes são alvos mais difíceis, os países acordaram na Cimeira de Varsóvia sete requisitos chave para aumentar a resiliência: (i) assegurar a governabilidade e serviços críticos governamentais, (ii) resiliência do setor energético, (iii) capacidade para lidar com fluxos migratórios não controlados, (IV) resiliência do bens alimentares e água, (V) capacidade para lidar com catástrofes com baixas numerosas, (VI) resiliência do sistemas de comunicações e (VII) resiliência do setor de transportes. Assim o foco na NATO incide, sobre a prevenção das AH dos países e nas suas civil preparedness[32], embora se mantenha apta à intervenção em larga escala através do mecanismo "Euro-Atlantic Disaster Response Coordination Centre".

Na última Cimeira da NATO[33], o Secretário-Geral além de manter uma tónica de continuidade sobre a tipologia das ameaças, como o terrorismo sob todas as suas formas e manifestações, alguns Estados e atores não estatais, expõe factos potenciadores das AH, como a instabilidade interna dos países e fenómenos migratórios. Salienta ainda o continuar dos trabalhos para aumentar a resiliência das sociedades, capacitando o Ciber, as infraestruturas críticas e a segurança do setor energético (NATO, 2019).

---

[28] Autores, como Fleming (2011), que referem que ameaças são adversários e, autores que referem que as AH são ações, como o Hybrid COE https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

[29] A Cimeira da NATO de Lisboa, em novembro de 2010, teve, como temas centrais a proliferação das armas de destruição maciça e o terrorismo, com o objetivo de reforçar a aliança transatlântica.

[30] Em Gales que teve como foco a segurança da região Euro-Atlântica devido às ações russas que vieram a desafiar a "(…) visão de uma Europa una, livre e pacífica (…) (NATO, 2014).

[31] Ocorrida em 08 e 09 de julho de 2016 e com a participação de Montenegro, pela primeira vez.

[32] *Civil Preparedness* significa o continuar das funções governativas básicas em casos de desastre ou emergências graves durante um período de paz ou crise. Representa a capacidade do setor civil para apoiar as operações militares da NATO. Está relacionado com a responsabilidade de ser resiliente, previsto no Art.º 3 do Tratado que contribui para a prevenção e CAH (NATO, 2018)

[33] Cimeira de Londres, em dezembro de 2019.

Apêndice C — Domínios do modelo conceptual para CAH do Hybrid CoE

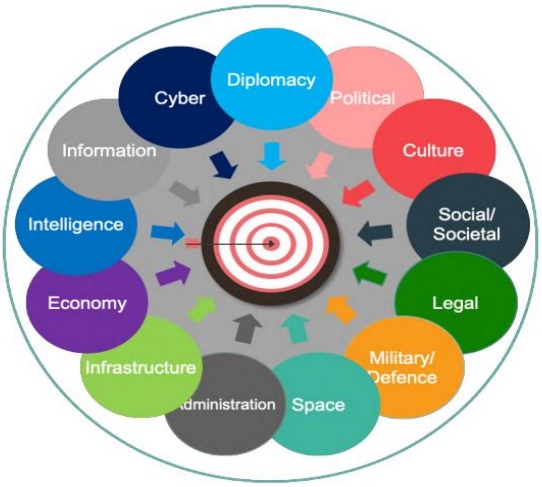

Figura 7 – Domínios das Ameaças Híbridas
Fonte: Adaptado de Schmid, J. (2019a) *Hybrid Warfare – a very short introduction*. *Concept Paper*, p. 7.

Na seleção dos domínios, Figura 7, o modelo conceptual teve em consideração que a generalidade dos conceitos para os instrumentos do poder nacional, tinham origem na vertente militar. De acordo com os pressupostos do modelo do Hybrid CoE, o controlo substancial por um ator sobre o objetivo, pode ser alcançado sem envolvimento de atividade militar e ocupação territorial. Atualmente, não existe prevalência à estruturação de instrumentos do poder nacional, nem lógica para selecionar um conceito rígido de instrumentos de poder face à multiplicidade de abordagens que são utilizadas em paralelo, nem devem ser observados de modo isolado, tendo identificado treze (13) domínios que projetam a complexidade da atividade coordenada da AH (Hybrid CoE, 2020).

1. Infraestruturas

Embora não exista uma definição transversalmente aceite de infraestruturas críticas, todas as definições enfatizam o seu papel para a sociedade, ou o seu efeito debilitante no caso de uma perturbação.

Uma definição europeia classifica "infraestruturas críticas" como "Um bem, sistema ou parte dele localizado em EM, essencial para a manutenção das funções vitais da sociedade, saúde, segurança, bem-estar económico ou social de pessoas, e a perturbação ou destruição terá um impacto significativo num EM, como resultado da impossibilidade de manter essas funções" (Diretiva n.º 114/2008/CE, 2008, p.3.). Coloca-se assim o enfase ênfase na prestação de serviços essenciais e a sua continuidade, sendo exemplos sectores que incluem: Energia (eletricidade, petróleo e gás); Transporte (ferroviário, rodoviário, marítimo, aéreo); Media; Banca e Finanças; Saúde; Alimentação; Água; Indústria, Fronteiras, etc.

2. Ciber

A dimensão *ciber* desempenha atualmente um papel excecional e muito relevante relativamente às AH. Em termos de planeamento de segurança inclui a cibercriminalidade, a propaganda, a espionagem, a influência, o terrorismo e até mesmo a própria guerra. O ciberespaço assegura anonimato e indetetabilidade. Incide na interdependência das redes e infraestruturas, da tecnologia de informação (incluindo hardware, software, dados, protocolos), e na Internet, nas redes de telecomunicações, nos sistemas informáticos, e nos processadores incorporados e controladores. O ciberespaço é um domínio chave potenciador de ações noutros domínios de operações e tornou-se ele próprio uma área operacional[34].

A diretiva sobre segurança de redes e sistemas de informação (*NIS Directive*) (Markopouloua, 2019) destaca a forte ligação entre os domínios de infraestruturas e Ciber, ao centrar a cibersegurança, aplicada aos seguintes sectores de infraestruturas: Energia (eletricidade, petróleo e gás), Transportes (aéreos, ferroviários, hídricos e rodoviários), Banca (instituições de crédito), Infraestruturas do mercado financeiro (locais de

[34] A NATO reconheceu em julho de 2016 que o ciberespaço é um domínio de operações em que deve defender-se tão eficazmente como se defende no ar em terra e no mar (e até mesmo no espaço) (NATO 2018).

comércio, contrapartes centrais), Saúde (ambientes de cuidados de saúde), Água (abastecimento e distribuição de água potável), Infraestruturas digitais (pontos de troca na Internet, fornecedores de serviços de sistemas de nomes de domínios, registos de nomes de domínios de primeiro nível).

3. Espaço

Os serviços baseados no domínio espaço incluem a navegação, as comunicações, a teledeteção, e ciência e exploração. Existe uma crescente preocupação com as atividades híbridas no espaço, uma vez que as operações híbridas no espaço não afetam apenas o domínio militar, mas também podem ter impacto nas atividades comerciais civis uma vez que estes dependem cada vez mais das capacidades espaciais. De facto, a maioria das ferramentas que podem visar o domínio espacial explora a ligação do espaço com os outros domínios do CAH considerados no modelo e, os potenciais efeitos em cascata, com forte ligação com o domínio militar, economia, infraestruturas, informação e informações (Hybrid CoE, 2020).

4. Economia

A economia como um domínio da AH é interpretada como a produção, a distribuição e o consumo de todos os bens e serviços de um país, e inclui o seu desenvolvimento económico e distribuição de riqueza (NATO, 2013). Na sociedade globalizada de hoje, as relações económicas são inerentemente suscetíveis à manipulação estatal, e são rotineiramente exploradas por vários países como meio de primeiro recurso para fins estratégicos. Instrumentos de política económica tais como sanções, tributação, embargos, acordos comerciais, congelamento de bens, intervenções esterilizadas, subsídios, tarifas, empréstimos soberanos e perdão da dívida são todos utilizados neste contexto. A economia tem sido considerada desde há muito um instrumento de guerra tradicional, mas destinava-se a apoiar o esforço de guerra (NATO 2013).

As atividades híbridas que procuram afetar a economia são suscetíveis de incluir iniciativas, incentivos e sanções concebidas para afetar o fluxo de bens e serviços, bem como apoio financeiro a atores estatais e não estatais, de uma forma que apoie os objetivos estratégicos do agressor (Hybrid CoE, 2020).

5. Militar e Defesa

Nas operações militares, a tarefa dos militares é preservar a independência, bem como a inviolabilidade e unidade do território nacional, particularmente para a manutenção e defesa da soberania. Em tempos de paz, os militares juntam-se às autoridades civis para fins de exercícios e assistência. As capacidades militares e de defesa de um país constituem uma pedra angular da sua própria existência e projeção de poder, sendo as capacidades militares uma condição prévia para que um país seja visto como um ator importante na arena geopolítica global.

A atividade relacionada com a AH terá como objetivo afetar as formas e os meios dos militares do país alvo, o que significa que a atividade procurará minar qualquer pensamento estratégico, procedimentos e práticas que estejam ligados aos militares, bem como às tropas, sistemas de armamento, etc. (Hybrid CoE, 2020). O domínio militar/de defesa está estreitamente ligado aos domínios cibernético, económico, espacial, cultural, social, de infraestruturas e diplomacia. O domínio militar é, evidentemente, central se a atividade híbrida se intensificar para o nível de coerção.

6. Cultural

Este domínio implica a utilização de cultura por um agressor para apoiar um objetivo através de uma atividade híbrida. A utilização deste domínio pode processar-se interna e externamente. Internamente, envolve a utilização de temas culturais e civilizacionais num esforço para definir elementos fundamentais de uma identidade nacional, enquanto estratégia de política externa, procura promover a cultura como meio para projetar uma imagem atrativa exterior.

Dada a natureza das ameaças híbridas, o domínio cultural implica principalmente uma estratégia de política externa. Neste sentido, pode procurar projetar uma imagem positiva do adversário híbrido no Estado alvo, uma imagem negativa do Estado alvo e dos seus aliados no estrangeiro, ou semear o desacordo e o caos no seio da respetiva sociedade (Hybrid CoE, 2020).

7. Social

O domínio social inclui áreas da sociedade que podem ser exploradas por um adversário híbrido ao procurar gerar, aprofundar ou explorar clivagens socioculturais, que gerarão a agitação social necessária para que uma atividade híbrida prossiga ou tenha sucesso. Questões controversas como o desemprego, a pobreza e a educação, são alvo fácil nas sociedades ocidentais. Acrescem as questões particularmente atrativas, como a recessão económica, a imigração irregular e ataques terroristas. O objetivo final será influenciar a forma como a sociedade trabalha no estado alvo para criar condições favoráveis a uma atividade híbrida e incutir medo na população, minar a sua confiança no governo, ou podem tentar polarizar a sociedade e promover a agitação social. Incluem assim tentativas de manipulação das perceções das pessoas, exploração de clivagens sociais (por exemplo, relativas à religião ou etnia), exploração da migração para aprofundar clivagens, e interferência nos meios de comunicação social (Hybrid CoE, 2020).

8. Administração Pública

A administração pública é interpretada no seu sentido mais amplo como o processo de traduzir políticas públicas em resultados. A dicotomia política-administração é enfatizada como uma característica

fundamental das sociedades europeias, existindo para implementar a lei. A administração em sociedades abertas e democráticas está organizada de uma forma que procura equilibrar a necessidade de manter a dicotomia política-administração com a necessidade de melhorar a coordenação e a eficiência. No entanto, a separação de poderes, os controlos e equilíbrios, e a estrutura institucional podem complicar as ações para mitigar as ameaças híbridas. Os instrumentos deste domínio estão diretamente relacionados com os problemas organizacionais inerentes aos governos democráticos (Hybrid CoE, 2020).

9. Legal

O domínio jurídico refere-se ao agregado de normas, ações, processos e instituições legais, incluindo a sua manifestação normativa e física, que são ou podem ser utilizados para alcançar efeitos legais ou não legais no contexto de uma campanha híbrida. Os adversários utilizam a lei como componente integral de atividades híbridas, utilizando uma vasta gama de ferramentas legais para apoiar uma campanha híbrida, incluindo a exploração de limiares legais, lacunas, complexidade e incerteza; contornar as suas obrigações legais; evitar a responsabilização; alavancar o cumprimento das regras pelo Estado visado; explorar a falta de interoperabilidade legal entre Nações visadas; utilizar os seus próprios poderes reguladores ao abrigo do direito interno; e utilizar a lei e os processos legais para criar narrativas e contra narrativas. Embora algumas destas táticas possam envolver violações das regras aplicáveis do direito nacional ou internacional, nem todas o fazem (Hybrid CoE, 2020).

10. Informações

As Informações são um processo pelo qual tipos específicos de informação importantes para a segurança nacional são solicitados, recolhidos, analisados e fornecidos aos decisores políticos; os produtos desse processo; a salvaguarda desses processos e dessa informação através de atividades de contraespionagem; e a realização de operações conforme solicitado pelas autoridades legais. O objetivo do domínio de Informações nas atividades híbridas, quer seja utilizado para implementar operações clandestinas de apoio a atividades híbridas ou para desfocar a consciência situacional do Estado alvo, é minar as capacidades de tomada de decisão a nível político e a capacidade da administração pública para implementar políticas (Hybrid CoE, 2020).

11. Diplomacia

A diplomacia é interpretada como a condução das relações internacionais, sendo que as suas teorias normativas justificam a guerra como medida defensiva contra a agressão provocada, sujeita às restrições da proporcionalidade e da proteção dos não combatentes. Fora esta exceção, a soberania do Estado é considerada quase sagrada na teoria das relações internacionais, pelo que a intervenção nos assuntos internos de outro País só pode ser justificada por razões humanitárias. As atividades híbridas, especialmente no domínio da diplomacia, são concebidas para minar a tomada de decisões e a unidade de ação, através de instrumentos utilizados neste contexto, incluindo sanções diplomáticas, boicotes, o uso de embaixadas e a criação de narrativas confusas ou contraditórias (Hybrid CoE, 2020).

12. Político

No contexto das AH, o domínio político abrange os atores, organizações e instituições que exercem autoridade ou governam num território através da aplicação de várias formas de poder e influência política (NATO 2013). Um adversário híbrido pode tentar explorar o domínio político para influenciar o Estado alvo ou estabelecer condições favoráveis para a realização de uma atividade híbrida, utilizando o poder político quer dentro de um país, quer na arena diplomática.

Os instrumentos deste domínio visam processos democráticos, organizações políticas e pessoas. Alguns instrumentos do domínio político tentam mudar a perceção do público sobre as escolhas políticas e/ou os atores, pelo que os instrumentos do domínio da informação podem ser utilizados para apoiar atividades híbridas que procuram explorar o domínio político (Hybrid CoE, 2020).

13. Informacional

A instrumentalização do domínio informacional continua a ser indiscutivelmente a marca registada das AH e das estratégias não lineares. É utilizada para minar a perceção da segurança do povo, colocando identidades políticas, sociais e culturais umas contra as outras.

O objetivo do adversário híbrido é explorar políticas e lealdades de identidade, dividindo assim grupos de interesse influentes e alianças políticas. Em virtude da sua baixa intensidade e potencial de negação, as atividades híbridas concebidas para explorar este domínio são geralmente de baixo risco, permitem uma abordagem de tentativa e erro, e têm um custo relativamente baixo, sendo algumas mesmo abertas à externalização. A desinformação ciber, propaganda e noticias falsas procuram mudar o discurso político, criar ou promover narrativas, e manipular a opinião pública e os sentimentos e podem prejudicar a liberdade de opinião e de expressão (Hybrid CoE, 2020).

Apêndice D — Ferramentas da atividade híbrida do Hybrid CoE

Quadro 14 - Ferramentas da atividade híbrida

Ferramenta	Descrição	Domínio afetado
Operações físicas contra infraestruturas	As operações físicas contra infraestruturas podem incluir intervenção terrorista, sabotagem ou vandalismo com o objetivo de destruir, perturbar ou sobrecarregar uma infraestrutura. Tais operações podem relacionar-se com infraestruturas nacionais chave e por isso incluídas nesta secção. Exemplos de utilização potencial incluem: - sabotagem contra centrais nucleares, instalações industriais químicas, laboratórios biológicos em hospitais e empresas privadas de biotecnologia; - ataques terroristas contra centros de transporte e espaços públicos; - contaminação de recursos hídricos e alimentares; ações contra a infraestrutura fronteiriça.	Infraestruturas, Economia, Ciber, Espaço, Militar e Defesa, Informacional, Social, Administração Publica
Criar e explorar dependências em infraestruturas (incluindo dependência civil-militar)	O exemplo mais proeminente desta ferramenta é a dependência energética. Esta ferramenta pode: - Manipular a política de preços do fornecimento de energia a países terceiros. - Controlando bens energéticos em países-chave. - Cortar ou interromper o fornecimento. - Acordar contratos de fornecimento restritivos. - Desenvolver rotas de abastecimento alternativas para desviar fluxos. Ameaças à interrupção do fornecimento é forma de exploração.	Infraestruturas, Economia, Ciber, Espaço, Militar e Defesa, Administração Pública
Criar e explorar dependências económicas	Embora a teoria económica enfatize os benefícios do comércio internacional, este último pode também gerar externalidades de segurança significativas, principalmente através da criação de dependências económicas. Dependências sobre mercadorias importadas e/ou exportadas, podem aumentar a vulnerabilidade à coerção através do comércio internacional.	Economia, Diplomático, Político, Administração Publica
Investimento direto estrangeiro	A maioria das infraestruturas críticas são de propriedade privada. Embora a privatização tenha criado maior concorrência, melhores serviços e preços mais baixos para os cidadãos, ao mesmo tempo levanta preocupações no que diz respeito à segurança e resistência destas infraestruturas. O estatuto de propriedade de infraestruturas críticas está a receber muita atenção a nível político, e os atos legislativos (sobre o Investimento Direto Estrangeiro) podem ser um instrumento útil para reduzir o risco associado às infraestruturas energéticas e ao aprovisionamento energético da UE, bem como o esquema de propriedade dos Sistemas Autónomos que constitui a espinha dorsal da Internet.	Economia, Infraestruturas, Ciber, Espaço, Militar e Defesa, Administração Publica, Informações, Informacional, Político, Legal
Espionagem industrial	São vários os alvos potenciais de espionagem industrial por estados estrangeiros, como energia/alternativa, biotecnologia, tecnologia de defesa, proteção ambiental, fabrico de alta qualidade e tecnologia de informação e comunicação. Para além das ferramentas cibernéticas para a adquirir, know-how ou vantagem estratégica, as ferramentas alternativas podem incluir: a utilização de *joint ventures*, fusões e aquisições, empresas de fachada, investigação e colaborações académicas, ou programas de recrutamento de talentos.	Economia, Infraestruturas, Ciber, Espaço, Informações, Informacional
Minar a economia nacional do adversário	A tentativa de enfraquecer a economia de um adversário não é uma novidade no arsenal económico do Estado. Embora ostensivamente interpretadas como retaliação por violações do direito internacional, as sanções também podem ser aplicadas com a intenção de enfraquecer a economia e, eventualmente, afirmar a força do país que aplica as sanções. Embargos, tarifas e outras medidas também podem fazer parte de uma estratégia híbrida mais ampla, que pode incluir outros instrumentos no domínio da economia.	Economia, Administração Publica, Político, Diplomático
Alavancagem de dificuldades económicas	As dificuldades económicas existentes geram vulnerabilidades às AH. O baixo desenvolvimento económico e a incapacidade de assegurar o financiamento dos mercados apresentam oportunidades para os adversários híbridos. Uma economia fraca é mais fácil de afetar negativamente. O crescimento lento, a recessão e/ou a dívida soberana podem ser instrumentos na medida em que minam a legitimidade do governo e retratam a imagem de um estado falido.	Economia, Administração Publica, Político, Diplomático
Ciber espionagem	A disponibilidade de novas ferramentas ciber mudou o carácter da espionagem e ofereceu um recurso de baixo risco e custo, mas de resultados significativos. Referem-se ataques e fugas visando as infraestruturas eleitorais e uma gama diversificada de atividades comerciais, indústrias e tecnologias, incluindo aviação, tecnologia de satélite e marítima, automação de fábricas industriais, fornecimentos para automóveis, instrumentos de laboratório, bancos e finanças, telecomunicações e eletrónica de consumo, tecnologia de processamento de computadores, serviços de tecnologia da informação, embalagem, consultoria, equipamento médico, cuidados de saúde, biotecnologia, fabrico de produtos farmacêuticos, mineração, exploração e produção de petróleo e gás.	Infraestruturas, Espaço, Ciber, Militar e Defesa, Administração Publica
Operações Ciber	As operações cibernéticas podem visar os dados e os bens que os utilizam, nomeadamente as antenas em satélites e estações terrestres,	Infraestruturas, Espaço, Ciber, Social,

	as linhas terrestres que ligam as estações terrestres às redes terrestres, e os terminais dos utilizadores que se ligam aos satélites, como potenciais pontos de intrusão. A maioria dos ataques ou operações cibernéticas referem-se a espionagem, mas existem crescentes preocupações com a manipulação dos dados e informações acedidas, nomeadamente desfiguração de websites, redireccionamento de domínios para sites controlados, roubo de correio eletrónico, e desvio de contas de comunicação social.	Administração Publica, Militar e Defesa
Violação do Espaço Aéreo	A violação do espaço aéreo é uma ferramenta amplamente utilizada no quadro de atividades híbridas. Podem ser vistas como uma forma de desafiar a soberania ou formalizar reivindicações e exercer pressão sobre um governo. A violação do espaço aéreo pode ser utilizada como um método de teste para medir o nível de resposta do adversário e a sua capacidade de realizar operações semelhantes.	Militar e Defesa, Social, Político, Diplomático
Violação das Águas Territoriais	A violação das águas territoriais é uma ferramenta que é utilizada de forma semelhante à violação do espaço aéreo. Devido à natureza desta ferramenta, as violações não podem exibir a mesma frequência e dinâmica, sendo consideradas mais graves devido às capacidades dos modernos navios de guerra em comparação com os aviões.	Militar e Defesa, Social, Político, Diplomático
Proliferação de Armas	A maioria dos países presta muita atenção à proliferação de armas de destruição maciça, contudo, no contexto das ameaças híbridas, a proliferação de armas convencionais (por exemplo, *manpads*, *drones*) e tecnologias é uma questão que tem sido largamente negligenciada. Deve ainda considerar-se a proliferação de tecnologias críticas relacionadas com o domínio militar.	Militar e Defesa
Operações militares convencional e não convencionais	A nova realidade das ameaças híbridas inclui a utilização de operações convencionais e não convencionais. As FFAA devem ser reorganizadas a fim de combater as chamadas batalhas multidomínio, que se caracteriza por adversários que não se declararão como inimigos, mas combinarão forças regulares e irregulares com empresas criminosas e terroristas para atacar as vulnerabilidades e evitando os pontos fortes.	Militar e Defesa
Organizações Paramilitares	As organizações paramilitares estão fortemente envolvidas em atividades híbridas em nome de um ator estatal, e empregam principalmente ações cinéticas. As organizações paramilitares estão, ativas durante as últimas fases da escalada de uma atividade híbrida, nomeadamente durante as fases de desestabilização/coerção ou mesmo de guerra. Oferecem negação, o que é essencial para uma série de atores estatais e enfraquecem a capacidade de atribuição.	Militar e Defesa
Exercícios Militares	Os exercícios militares podem ser um instrumento muito poderoso no quadro da atividade híbrida para a projeção de poder, intimidação e efeitos psicológicos exercidos sobre a população em geral. São uma ferramenta que pode ser utilizada durante toda a linha temporal de uma atividade híbrida. Para além do valor elevado dos exercícios, existe ainda o valor da mensagem como fator de dissuasão.	Militar e Defesa, Diplomático, Político, Social
Envolver as diásporas para influenciar	As diásporas podem tornar-se atores viáveis para efeitos da AH, quando as suas ações são manipuladas secretamente pelo governo do país anfitrião, a fim de influenciar o comportamento da pátria ou, inversamente, quando um governo da pátria pode explorar os sentimentos da diáspora para os seus propósitos. Este é um instrumento estratégico implementado tanto por regimes democráticos como autoritários, com política concebida como uma obrigação moral de proteger a diáspora.	Político, Diplomático, Social, Cultural, Informações, Informacional
Financiamento de grupos culturais e de reflexão	O financiamento de grupos extremistas através de associações culturais estabelecidas sob o pretexto de promover o património comum de países, financiamento para a criação de grupos de reflexão, muitas vezes através de empresas de fachada. O objetivo é influenciar a política através de uma entidade aparentemente independente.	Social, Cultural, Político, Diplomático
Exploração de clivagens socioculturais (étnicas, religiosas e culturais)	As clivagens socioculturais fornecem terreno fértil para um adversário híbrido explorar e criar tensão social, polarizar a sociedade, instilar medo na população ou minar a sua confiança no governo. As campanhas de desinformação visam frequentemente questões litigiosas. As questões com potencial para criar ou sustentar uma crise são particularmente atrativas e incluem a recente desaceleração económica, imigração irregular e ataques terroristas. A religião é um exemplo que um adversário híbrido pode procurar alavancar em questões socialmente sensíveis. As minorias fornecem frequentemente o fulcro para alavancar clivagens socioculturais, enquanto instrumentos em campanhas de desinformação.	Social, Cultura
Promover a agitação social	Um adversário híbrido pode tentar promover a agitação social para desestabilizar o governo de um país, gerar e explorar tensão social, ou encorajar um certo comportamento no país alvo. Se corretamente utilizado, este instrumento pode ser particularmente eficaz.	Infraestruturas, Social, Económico, Político
Manipular discursos sobre	A migração é particularmente suscetível à exploração como parte das AH. Um afluxo de imigrantes e refugiados pode desencadear	Social, Cultural, Político, Legal

migração para polarizar as sociedades e minar as democracias liberais	sentimentos na sociedade de acolhimento de ameaça social e económica. O objetivo final será interferir nos processos eleitorais e minar os fundamentos do apoio popular à democracia liberal como a forma ideal de organização política e social.	
Explorar as vulnerabilidades da Administração Publica (incluindo gestão de crises)	Regulamentos imaturos, capacidades de monitorização limitadas, uma função pública sem experiência e sem profissionalismo, e um aparelho governamental débil, são vulnerabilidades críticas que os adversários híbridos podem explorar. A economia, as infraestruturas, e a elaboração e implementação de leis e políticas podem ser adversamente afetadas por um aparelho governamental que funciona mal. Enfraquecer as capacidades de gestão de crises, pode aumentar a frequência e o custo das catástrofes para o Estado alvo. Desastres graves, catástrofes ou perdas recorrentes podem minar a confiança nas instituições governamentais e oportunidades de desinformação destinadas a desestabilizar o governo.	Administração Publica, Político, Social
Promover e explorar a corrupção	Para além das questões organizacionais decorrentes de conflitos entre organismos, a corrupção é ainda outro problema. A corrupção cria vulnerabilidades à AH, ao restringir a eficiência do aparelho governamental e ao minar a tomada de decisões.	Administração Publica, Economia, Legal, Social
Exploração de limites pouco claros, lacunas e ambiguidade da lei	Os adversários podem conduzir deliberadamente atividades híbridas abaixo de certos limiares legais críticos, em particular os que regem o uso da força. Isto permite aos conselheiros evitar as consequências legais e práticas que a ultrapassagem destes limiares implicaria. Operações híbridas que atingem o nível de um ataque armado desencadeiam o direito de autodefesa e permitem que a nação visada responda com força militar. Acresce que tais operações podem também envolver os compromissos de assistência mútua da NATO e da UE, ambos operacionalizando o direito de autodefesa.	Infraestruturas, Ciber, Espaço, Economico, Militar e Defesa, Cultura, Social, Administração Publica, Legal, Informações, Diplomacia, Político, Informacional
Alavancar argumentos, regras legais, processos, e instituições	Os consultores podem utilizar regras legais, processos, instituições e argumentos tanto a nível nacional como internacional em apoio de campanhas híbridas. Nesses casos, a lei e o cumprimento continuado da lei por parte dos Estados e sociedades visados é utilizado como alavanca contra estes. Por exemplo, os regulamentos nacionais relativos à propriedade intelectual, aos meios de comunicação social, à tecnologia e domínios afins podem ser utilizados em apoio à atividade híbrida. As tecnologias cibernéticas e de telecomunicações podem apresentar oportunidades semelhantes.	Infraestruturas, Ciber, Espaço, Economia, Militar e Defesa, Cultura, Social, Administração Publica, Legal, Informações, Diplomático, Político, Informacional
Sistemas de Informações	As atividades híbridas requerem uma compreensão profunda das vulnerabilidades dos Estados. Um adversário híbrido é suscetível de utilizar as Informações para obter uma compreensão do estado alvo no contexto do ambiente estratégico, antes e durante a implementação de atividades híbridas. Embora o adversário híbrido utilize os seus próprios serviços de informações, estas podem também ser recolhidas por procuração, desde estados organizados e organizações paramilitares, a partidos políticos, movimentos de protesto ou outros grupos sociais.	Informações, Militar e Defesa
Operações Clandestinas	As informações são, por natureza, melhores se mantidas em segredo, pelo que as agências de informações desenvolvem e mantêm as suas capacidades de planear e conduzir operações clandestinas. Embora destinadas principalmente à recolha de informações, estas capacidades também podem apoiar atividades híbridas.	Informações, Militar e Defesa
Infiltração	Para além da tradicional recolha de informações e operações clandestinas, um adversário híbrido pode tentar infiltrar-se em organizações críticas do Estado alvo, para manipular pessoas de influência, tais como políticos, jornalistas, académicos e formadores de opinião.	Informações, Militar e Defesa
Sansões Diplomáticas	Sanções diplomáticas, são medidas implementadas por um país ou organização internacional como parte do seu esforço diplomático para estimular uma mudança de política num outro país. Podem incluir embargos de armas, proibições de viagens, congelamento de bens, sanções económicas e a redução ou supressão dos laços diplomáticos.	Diplomático, Político, Economico
Boicotes	Os boicotes podem ter um efeito semelhante aos embargos ou outras sanções económicas. No contexto das AH, o objetivo de um boicote é obrigar um Estado a alinhar-se com interesses, podendo ser impostos por governos, por empresas privadas e atores não estatais.	Diplomático, Político, Economico
Embaixadas	O adversário híbrido pode utilizar a sua própria rede de embaixadas para apoiar atividades híbridas ou tentar explorar a falta de representação diplomática do Estado alvo numa área. No contexto de AH, as embaixadas podem ser utilizadas para aplicar pressão diplomática e como centros locais de comando, controlo e coordenação de atividades de informações e operações clandestinas.	Diplomático, Político, Informações, Social

Criar confusão ou narrativas contraditórias	No contexto de AH, as narrativas podem ser utilizadas para múltiplos fins. Um adversário híbrido pode empregar narrativas contraditórias para criar confusão e minar os processos de tomada de decisão no estado alvo. Diferentes fontes podem também ser utilizadas para cada narrativa conflituosa, sendo um desafio à tomada de decisões em crises e mantendo o foco na "adivinhação". As narrativas públicas podem ainda ser utilizadas para justificar as ações de um adversário híbrido.	Social, Informacional, Diplomático
Migração como um moeda de troca em relações internacionais	A atenção aos movimentos de populações assume-se como uma questão de relações entre Estados no âmbito da segurança e estabilidade. Ameaças de encaminhar um elevado número de migrantes para outro país, para acomodar fluxos de refugiados ou migrantes, visa alcançar objetivos políticos. A migração pode ser vista como uma ferramenta da AH quando os governos a utilizam como estratagema de negociação para ganhos financeiros ou outros objetivos geopolíticos.	Social, Diplomático, Político
Desacreditação de lideranças e/ou candidatos	Desacreditar a liderança do Estado alvo e/ou os candidatos a cargos públicos oferece ao adversário híbrido múltiplas vantagens. Este descrédito é muitas vezes tentado por meio de detração, geralmente através das redes sociais em atividades de desinformação, ou divulgando informação privada, sensível ou mesmo classificada.	Político, Administração Publica, Social
Apoio a atores políticos	Para além de se opor aos líderes e/ou candidatos a cargos públicos de um Estado alvo, um adversário híbrido pode tentar apoiar os atores políticos favoráveis aos seus objetivos. Este apoio pode incluir a oposição aos seus oponentes e a prestação de apoio direto, tal como o financiamento, formação ou aconselhamento.	Político, Administração Publica, Social
Coerção de políticos e/ou governo	A coerção de políticos e/ou funcionários governamentais também pode ser utilizada por um adversário híbrido para apoiar a sua atividade. A coerção ocorre através de chantagem, ameaças ou outras formas de exercer pressão.	Político, Administração Publica, Legal
Exploração da imigração para influência política	A imigração é uma questão politizada e utilizada por atores híbridos, incitando ou facilitando os movimentos migratórios ou explorando a sua ocorrência através da utilização dos instrumentos de desinformação para influenciar o discurso político.	Político, Social
Controlo e influência do Media	Os meios de comunicação social são motores da informação pública e desempenham um papel importante na formação da opinião pública em relação às políticas, governos, estados e questões. Tentativas de ganhar o controlo dos meios de comunicação social no estado alvo estão entre as manifestações de AH em evolução. As tentativas de controlar os meios de comunicação social são orientadas para influenciar a opinião pública, apoiando as campanhas de desinformação e limitando o acesso a informação.	Informacional, Infraestruturas, Social, Cultural
Campanhas de desinformação e propaganda	As campanhas de desinformação com origem em fontes internas, podem não implicar necessariamente AH. No contexto das AH, a desinformação é semelhante à propaganda, uma forma de operações psicológicas. Um adversário híbrido pode usar a desinformação para apoiar os seus esforços subversivos e minar a política do Estado alvo, corroer a confiança dos cidadãos nas instituições e nos meios de comunicação social, e prejudicar a sua capacidade de tomar decisões informadas. Os esforços visam polarizar os debates, minar os sistemas e processos eleitorais, e criar novas ou aumentar as clivagens sociais e políticas existentes.	Social, Informacional, Político, Ciber, Cultural, Administração Publica
Influência curricular e académica	A tentativa de influenciar a escola e o ensino é uma ferramenta com uma visão a longo prazo. O objetivo do adversário híbrido é infundir elementos da sua cultura na cultura do Estado alvo e tornar a população do estado alvo mais. Se uma minoria do ator híbrido existir ou for estabelecida no Estado alvo, afetando o conteúdo ou forma de educação pode perturbar a homogeneidade social.	Social, Cultural
Operações eletrónicas (interferência de GNSS e falsificações)	Visam a interferência ou falsificação de sinais de radiofrequência. Devido ao seu baixo custo e dependência do GNSS, o risco de ataques maliciosos utilizando interferências radioelétricas é cada vez mais crítico, sendo a interferência mais significativa a conduzida por atores com capacidades de empastelamento de armas guiadas por GNSS, como os UAV (*drones*) e mísseis guiados. Realce ainda para as redes de distribuição da rede elétrica, redes de telecomunicações terrestres 4G e 5G, redes financeiras, e toda a gama de sistemas de transporte (aéreo, marítimo, ferroviário e rodoviário), que dependem do GNSS. Um ataque malicioso de negação de serviços GNSS pode levar a uma grande perturbação em serviços críticos tais como eletricidade, serviços bancários, comunicações sem fios de banda larga, ou operações de transporte aéreo ou marítimo. A interferência maliciosa, falsificação, intrusão ou interceção de sinal de comunicações via satélite são exemplos de ataques que representam uma séria ameaça.	Espaço, Ciber, Infraestruturas, Económico, Militar e Defesa

Fonte: Adaptado de Hybrid CoE (2020)

Apêndice E — Personalidades consideradas para entrevistas

As entrevistas dirigidas a entidades especialistas na matéria, que se constituem como uma amostra do tipo não probabilística ou empírica, intencional (Santos L. &., 2019), foram estruturadas em dois grupos. Um primeiro grupo de quatro entrevistas, a representantes de organismos centrais do estado e representantes dos diferentes domínios de poder e, um segundo grupo de 13 entrevistas a estudiosos de reconhecida competência na matéria em estudo, num total de 17 entrevistas, recorrendo à plataforma de vídeo conferência TEAMS e por email, no período de novembro a março.

Quadro 15 - Entrevistas

	ORGÃO	IDENTIFICAÇÃO	DATA
Entrevistas Exploratórias	DGPE/MNE	Embaixador Jorge Aranda	04NOV20
	DGPDN/MDN	Cmdt Frag Guerreiro de Oliveira	O3NOV20
	ISCPSI	Dr. Pathe Duarte	17NOV20
	IUM	Maj Art Lourenço Serrão	27OUT20
1º Grupo de Entrevistas Semiestruturadas	SG SSI	Cor Óscar Nascimento Rocha	06FEV21
	GNS	CALM Gameiro Marques	10FEV21
	SIED	Quadro Dirigente	02MAR21
	IUM	Maj Art Lourenço Serrão	09MAR21
2º Grupo de Entrevistas Semiestruturadas	UCP	Dr. (TCor) Proença Garcia	04FEV21
	ISCPSI	Dr. Pathe Duarte	08FEV21
	AM	Cor Viegas Nunes	10FEV21
	IUM	TCor Moutinho Fernandes	10FEV21
	DGPDN/MDN	Cmdt Frag Guerreiro de Oliveira	11FEV21
	DGPDN/MDN	BGen Lemos Pires	15FEV21
	MINUSCA	MGen Maia Pereira	15FEV21
	CPHM	MGen Vieira Borges	18FEV21
	DIPLAEM/EMGFA	BGen Rui Ferreira	19FEV21
	Corpo Fuzileiros	CMG Mariano Alves	22FEV21
	Dir Coord EME	MGen Eduardo Ferrão	01MAR21
	CEMCCOM/EMGFA	TGen Marco Serronha	01MAR21
	Planeamento cenários GH – ACT / SHAPE	Dr. Manuel Poêjo Torres	11MAR21
Entrevistas de Confirmação	DGPE/MNE	Embaixador Jorge Aranda	08ABR21
	Dir Coord EME	MGen Eduardo Ferrão	13ABR21
	GNS	CALM Gameiro Marques	12ABR21
	Planeamento cenários GH – ACT / SHAPE	Dr. Manuel Poêjo Torres	14ABR21

Apêndice F — Estrutura base dos blocos das entrevistas semiestruturadas

Guião do 1º Bloco de entrevistas semiestruturadas

Caracterização do entrevistado
Entrevista n.º _____
Nome do entrevistado: _____
Ramo: _____Posto_____Classe:_____ Cargo: _____
Local: _____Data: _____

Excelentíssimo Senhor,

Chamo-me António José Ruivo Grilo, Coronel de Artilharia, e sou Auditor do Curso de Promoção a Oficial-General (CPOG) 2020/2021, que decorre no Instituto Universitário Militar (IUM).

Durante este curso, os auditores elaboram Trabalhos de Investigação Individual (TII), em que se abordam questões relevantes e importantes para o futuro das FFAA e da Defesa Nacional. Neste âmbito, encontro-me a realizar uma investigação com o seguinte enunciado: "*A Defesa Nacional na Prevenção e Combate às Ameaças Híbridas*". O objetivo geral deste TII consiste em propor linhas de ação estratégicas no âmbito da Defesa Nacional para o Combate às Ameaças Híbridas (CAH).

A metodologia seguida no TII segue uma estratégia de investigação qualitativa através da pesquisa e análise documental de referência e com recurso a entrevistas semiestruturadas, que são efetuadas a especialistas conhecedores do tema ou que tenham responsabilidades na área.

Solicito a sua autorização para gravar a presente entrevista e para referir no trabalho o conteúdo da mesma associado ao seu nome. Caso não seja essa a sua vontade, garanto a confidencialidade do entrevistado e tratarei a informação recolhida de forma anónima. Estimo que a entrevista dure um máximo de 20 minutos. O seu conhecimento e experiência são essenciais para a qualidade e relevância deste trabalho, pelo que, agradeço mais uma vez a sua disponibilidade para a prossecução da presente investigação.

Nestes termos gostaria de lhe colocar um conjunto de questões, cujas respostas serão fundamentais para identificar medidas nacionais passíveis de integrar a abordagem estratégica à AH.

Enquadramento:

O modelo conceptual, do Hybrid CoE (2019), *The Landscape of Hybrid Threats: A Conceptual Model*, foi desenvolvido pela UE em dezembro de 2019, pretende apoiar as Nações na definição de estratégias nacionais para a prevenção e combate das AH.

O modelo conceptual apresenta domínios e ferramentas no CAH, para a conceção das ações certas a fim de enfrentar as AH, devendo ser considerado como um ponto de referência para os decisores políticos, a fim de conceber políticas e ações eficazes e eficientes, especialmente quando se trata de deteção e questões de atribuição.

Para dar continuidade ao TII, importa analisar o ambiente externo, identificando as principais ameaças e oportunidades para Portugal.

1ª Questão: Sabendo que a génese de todo o processo se situa no patamar estratégico, quais as das ferramentas do CAH que identifica como **ameaças mais prováveis e críticas para** Portugal, **no ambiente externo** suscetíveis de integrar uma abordagem estratégica nacional de combate à AH? Solicita-se uma avaliação de 1 a 6, sendo 1 muito critica e 6 pouco critica.

Muito Pouco

Ameaças Híbridas consideram-se ações coordenadas e sincronizadas que visam deliberadamente afetar as vulnerabilidades dos Estados democráticos e das suas instituições, empregando um leque particularmente amplo de meios políticos, económicos, militares, civis e de informação (Hybrid CoE, 2019).

Ferramenta	Grau de Ameaça (1 a 6)
1. Operações físicas contra infraestruturas	
2. Criar e explorar dependências em infraestruturas (incluindo dependência civil- militar)	
3. Criar e explorar dependências económicas	
4. Investimento direto estrangeiro	
5. Espionagem industrial	
6. Minar a economia nacional do adversário	
7. Alavancagem de dificuldades económicas	
8. Ciberespionagem	
9. Operações Ciber	
10. Violação do Espaço Aéreo	
11. Violação das Aguas Territoriais	
12. Proliferação de Armas	
13. Operações militares convencional e não convencionais	
14. Organizações Paramilitares	
15. Exercícios Militares	
16. Envolver as diásporas para influenciar	
17. Financiamento de grupos culturais e de reflexão	

18. Exploração de clivagens socioculturais (étnicas, religiosas e culturais)	
19. Promover a agitação social	
20. Manipular discursos sobre migração para polarizar as sociedades e minar as democracias liberais	
21. Explorar as vulnerabilidades da Administração Publica (incluindo gestão de crises)	
22. Promover e explorar a corrupção	
23. Exploração de limites pouco claros, lacunas e ambiguidade da lei	
24. Alavancar argumentos, regras legais, processos, e instituições	
25. Sistemas de Informações	
26. Operações Clandestinas	
27. Infiltração	
28. Sansões Diplomáticas	
29. Boicotes	
30. Embaixadas	
31. Criar confusão ou narrativas contraditórias	
32. Migração como uma moeda de troca em relações internacionais	
33. Desacreditação de lideranças e/ou candidatos	
34. Apoio a atores políticos	
35. Coerção de políticos e/ou governo	
36. Exploração da imigração para influência política	
37. Controlo e influência do Media	
38. Campanhas de desinformação e propaganda	
39. Influência curricular e académica	
40. Operações eletrónicas (interferência de GNSS e falsificações)	

2ª Questão: Para as ameaças mais críticas que classificou com a numeração um (1), solicita-se a identificação de **oportunidades externas que se identifiquem para Portugal**, suscetíveis de integrar uma abordagem estratégica nacional de combate à AH?

Oportunidades face a uma ameaça, são os caminhos ou espaço para crescimento, que podem ser desenvolvidos para suprir necessidades. Em outras palavras, são aspetos externos positivos, que quando utilizado em conjunto com o que a organização tem de positivo internamente, podem ser transformados em oportunidades de melhoria (Dias, Varela, & Costa, 2013).

Numero da Ameaças Criticas identificadas	Oportunidades
•	
•	
•	
•	

Guião do 2º Bloco de entrevistas semiestruturadas

Enquadramento:

Para dar continuidade ao TII, importa analisar o ambiente interno, identificando as principais potencialidades e vulnerabilidades para Portugal.

3ª Questão: Sabendo que a génese de todo o processo se situa no patamar estratégico, para cada um dos domínios da AH, quais as **potencialidades no ambiente interno que identifica para Portugal**, suscetíveis de integrar uma abordagem estratégica nacional de combate à AH?

Potencialidades são os pontos positivos, aspetos em que a organização se destaca internamente e que constituem uma vantagem face a outras organizações (Dias et al., 2013).

4ª Questão: Sabendo que a génese de todo o processo se situa no patamar estratégico, para cada um dos domínios da AH, quais as **vulnerabilidades no ambiente interno que identifica para Portugal**, suscetíveis de integrar uma abordagem estratégica nacional de combate à AH?

Vulnerabilidades, são os pontos negativos, desvantagens nacionais em relação a outros países, principais erros já cometidos, o que já foi reconhecido com um problema ou erro (Dias et al., 2013).

Domínios	Potencialidades	Vulnerabilidades
• Politico		
• Económico		
• Militar e Defesa		
• Diplomático		
• Informacional		
• Infraestruturas		
• Ciber e Espaço		
• Cultural		
• Administração Pública		
• Legal		
• Social		
• Informações (Intel)		

Muito obrigado pelo seu importante contributo e disponibilidade.

António José Ruivo Grilo

Coronel de Artilharia

Apêndice G — Análise de resultados

1. Ameaças

Ameaças Criticidade Alta	Média	Moda	% da Moda
38. Campanhas de desinformação e propaganda	1,47	1	65
8. Cyberespionagem	1,53	1	71
9. Operações Cyber	1,53	1	65
37. Controlo e influência do Media	1,94	1	41
3. Criar e explorar dependências económicas	2,24	1	41
25. Sistemas de Informações	2,53	2	41
5. Espionagem industrial	2,59	1	29
26. Operações Clandestinas	2,94	2	35
Ameaças Criticidade Média	**Média**	**Moda**	**% da Moda**
34. Apoio a atores políticos	2,59	3	41
40. Operações eletrónicas (interferência de GNSS e falsificações)	2,65	3	35
19. Promover a agitação social	2,82	3	47
31. Criar confusão ou narrativas contraditórias	2,82	3	41
33. Desacreditação de lideranças e/ou candidatos	2,82	3	47
20. Manipular discursos sobre migração para polarizar as sociedades e minar as democracias liberais	2,88	3	76
35. Coerção de políticos e/ou governo	2,88	3	41
7. Alavancagem de dificuldades económicas	3,00	3	35
18. Exploração de clivagens socioculturais (étnicas, religiosas e culturais)	3,00	3	53
22. Promover e explorar a corrupção	3,00	3	53
4. Investimento direto estrangeiro	3,06	3	53
36. Exploração da imigração para influência política	3,12	3	71
6. Minar a economia nacional do adversário	3,18	3	59
21. Explorar as vulnerabilidades da Administração Publica (incluindo gestão de crises)	3,18	3	47
2. Criar e explorar dependências em infraestruturas (incluindo dependência civil- militar)	3,24	3	41
10. Violação do Espaço Aéreo	3,24	3	29
11. Violação das Águas Territoriais	3,24	3	29
27. Infiltração	3,29	4	35
1. Operações físicas contra infraestruturas	3,35	3	35
12. Proliferação de Armas	3,35	3	41
17. Financiamento de grupos culturais e de reflexão	3,35	3	59
23. Exploração de limites pouco claros, lacunas e ambiguidade da lei	3,35	3	35
28. Sansões Diplomáticas	3,41	3	47
30. Embaixadas	3,47	3	53
16. Envolver as diásporas para influenciar	3,59	3	53
32. Migração como uma moeda de troca em relações internacionais	3,59	3	47
14. Organizações Paramilitares	3,76	3	59
39. Influência curricular e académica	3,82	3	35
24. Alavancar argumentos, regras legais, processos, e instituições	3,88	3	41
29. Boicotes	3,88	3	29
Ameaças Criticidade Baixa	**Média**	**Moda**	**% da Moda**
13. Operações militares convencional e não convencionais	3,76	6	29
15. Exercícios Militares	4,29	5	29

Figura 8 – Grupos de Criticidade da Ameaça

2. Oportunidades

Domínios / Ameaças	Unidade de Registo Oportunidades	Entrevistas																Unidades de Enumeração	
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15	#16	#17		
Social Campanhas de desinformação e propaganda	1.1 Gestão de perceções e educação social	X				X	X		X	X						X	X		7	41%
	1.2 Comunicação estratégica	X				X	X		X	X	X	X	X			X	X	X	11	65%
	1.3 Cooperação internacional NATO/UE			X		X						X	X				X		4	24%
	1.4 Conhecimento situacional	X		X	X	X	X				X	X					X	X	9	53%
	1.5 Estrutura de monitorização e identificação da ameaça e risco			X		X				X							X	X	5	29%
	1.6 Estratégia de resiliência à desinformação e propaganda					X										X		X	3	18%
Infraestruturas Ciberespionagem e operações ciber	2.1 Estratégia de resiliência Ciber das Infraestruturas criticas	X				X			X	X	X	X	X			X	X		9	53%
	2.2 Estrutura de monitorização e identificação da ameaça e risco	X			X	X								X		X			5	29%
	2.3 Cooperação internacional NATO/UE		X			X	X					X	X	X		X	X		8	47%
	2.4 Conhecimento situacional				X				X		X	X		X		X	X		7	41%
	2.5 Reforço dos Serviços de Informação do Estado				X	X													2	12%
	2.6 Moldura legal e regulamentação da UE					X	X						X						3	18%
Informacional Controlo e influência dos Media	3.1 Conhecimento situacional			X	X					X	X	X							5	29%
	3.2 Cooperação internacional NATO/UE			X								X							2	12%
	3.3 Estrutura de monitorização e identificação da ameaça e risco			X	X					X	X	X							5	29%
	3.4 Estratégia de resiliência informacional			X														X	2	12%
	3.5 Comunicação estratégica																	X	1	6%
Económico Criar e explorar dependências económicas e espionagem industrial	4.1 Estratégia de resiliência económica em infraestruturas criticas					X	X				X	X					X	X	6	35%
	4.2 Reduzir dependências económicas e diversificar fontes				X	X	X										X		4	24%
	4.3 Mecanismos de regulação económica e controlo da UE					X							X					X	3	18%
	4.4 Desenvolver indústria e planos de investimento				X	X				X			X				X		5	29%
	4.5 Conhecimento situacional				X				X		X	X					X	X	6	35%
	4.6 Estratégia económica da UE e parcerias económicas												X						1	6%
Informações Sistemas de Informações e Operações clandestinas	5.1 Estratégia de resiliência em infraestruturas criticas					X		X				X							3	18%
	5.2 Desenvolvimento das FFAA em tecnologias de ponta e ciberdefesa							X											1	6%
	5.3 Cooperação internacional NATO/UE							X				X	X		X			X	5	29%
	5.4 Conhecimento situacional							X			X	X	X						4	24%
	5.5 Estratégia de resiliência em ciberdefesa										X	X	X		X			X	5	29%
	5.6 Comunicação estratégica										X	X							2	12%

Figura 9 – Unidades de registo e enumeração de oportunidades

3. Potencialidades

Domínio	Unidade Registo Potencialidades	Entrevistas																Unidades de Enumeração	
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15	#16	#17	
Político	1.1 Sistema político consolidado e estável	X	X	X	X			X					X	X	X			X	9	53%
	1.2 Posicionamento geopolítico e pertença à NATO e UE					X			X			X		X			X		5	29%
	1.3 Presidência portuguesa da UE									X									1	6%
	1.4 Criar sistema nacional de gestão de crises							X											1	6%
	1.5 Coesão nacional										X								1	6%
Económico	2.1 Inovação e indústrias tecnológicas digitais e ciências	X						X	X	X	X	X		X					7	41%
	2.2 Energias renováveis		X								X			X					3	18%
	2.3 Espaço UE de trocas comerciais e mercado económico				X	X	X					X	X		X		X		7	41%
	2.4 Turismo										X		X						2	12%
	2.5 Ligação às diásporas e espaço lusófono					X							X				X	X	4	24%
Militar e Defesa	3.1 Articulação FFAA e FFSS	X									X								2	12%
	3.2 Dispersão territorial e prontidão	X					X							X	X		X	X	6	35%
	3.3 Integração NATO, UE e participação missões ONU		X	X	X	X			X	X	X	X					X		9	53%
	3.4 Ciberdefesa e espaço							X					X						2	12%
	3.5 Capacidade de vigilância e controlo EEINP					X							X				X	X	4	24%
Diplomático	4.1 Diplomacia consolidada	X	X		X						X		X	X	X		X		8	47%
	4.2 Ligação CPLP e Lusofonia					X					X	X	X					X	5	29%
	4.3 Comunicação estratégica e diplomacia pública							X									X		2	12%
	4.4 Arco e ligação UE e NATO			X							X							X	3	18%
Informacional	5.1 Pluralidade e confiança na informação	X	X		X	X					X		X				X	X	8	47%
	5.2 Plataformas eletrónicas		X		X						X		X				X		5	29%
	5.3 Liberdade de imprensa					X						X							2	12%
	5.4 Comunicação estratégica							X											1	6%
Infraestruturas	6.1 Boas infraestruturas existentes	X			X								X						3	18%
	6.2 Planos Resiliência Infraestruturas							X	X		X						X	X	5	29%
	6.3 Infraestruturas abastecimento espaço europeu		X			X				X							X		4	24%
Ciber e Espaço	7.1 Cibersegurança		X		X			X			X							X	5	29%
	7.2 Estratégia resiliência ciber			X															1	6%
	7.3 centros de inovação e polos tecnológicos	X			X		X						X						4	24%
	7.4 Potenciar cibendefesa com NATO e UE					X					X						X		3	18%
	7.5 Espaço e posicionamento dos Açores													X				X	2	12%
Cultural	8.1 Identidade e Unidade Cultural	X		X			X		X	X	X			X	X			X	9	53%
	8.2 Sociedade plural e multicultural		X		X							X	X						4	24%
	8.3 Diáspora e diplomacia cultural					X											X		2	12%
	8.4 Resiliência cultural						X	X											2	12%
Administração Pública	9.1 Resiliência da Administração Pública	X																	1	6%
	9.2 Funcionalismo público estruturado e profissional		X																1	6%
	9.3 Modernização governativa e cidadania eletrónica				X	X					X		X	X					5	29%
	9.4 Saúde, Justiça e Educação gratuitos					X											X		2	12%
Legal	10.1 Separação poderes legislativo e judicial		X		X													X	3	18%
	10.2 Edifício jurídico consolidado	X																	1	6%
	10.3 Proximidade dos cidadãos à justiça					X					X								2	12%
	10.4 Reforma do sistema legal							X											1	6%
	10.5 Benefício disposições da UE											X	X						2	12%
Social	11.1 Unidade nacional e coesão social	X	X	X	X	X	X		X			X	X	X				X	11	65%
	11.2 Garantia direitos fundamentais e proteção necessitados				X	X		X			X			X			X		6	35%
	11.3 Liberdade religiosa				X														1	6%
Informações (Intel)	12.1 Sistema integrado de centralização Intel	X								X	X	X		X	X				6	35%
	12.2 Intercambio Intel com NATO e UE		X			X							X	X		X	X		6	35%
	12.3 Sistema de vigilância e alerta				X														1	6%
	12.4 Desenvolvimento IA							X											1	6%

Figura 10 – Unidades de registo e enumeração de potencialidades

4. Vulnerabilidades

Domínio	Unidade Registo Vulnerabilidades	Entrevistas																Unidades de Enumeração	
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15	#16	#17	
Político	1.1 Fragmentação Política		X		X						X								3	18%
	1.2 Falta consciencialização Ameaças e segurança			X						X		X	X	X	X			X	7	41%
	1.3 Falta estratégia coordenação transversal e gestão crises integrada					X	X	X	X	X		X		X	X		X		9	53%
Económico	2.1 Limitada competitividade económica e orçamental	X				X			X		X	X	X				X	X	8	47%
	2.2 Dependência externa especialmente em recursos energéticos		X	X		X					X		X	X			X		7	41%
	2.3 Economia de serviços				X			X						X	X				4	24%
Militar e Defesa	3.1 Falta Recursos Humanos	X	X		X						X		X						5	29%
	3.2 Falta de Investimento		X		X						X	X	X	X				X	7	41%
	3.3 Resposta a ameaças multidomínio e gestão crises			X	X	X							X		X		X		6	35%
Diplomático	4.1 Pouca representatividade	X			X			X					X					X	5	29%
	4.2 Elevada rotatividade de recursos humanos		X																1	6%
	4.3 Estratégia de cooperação e coordenação ameaças e riscos			X		X							X		X		X		5	29%
Informacional	5.1 Iliteracia Digital		X		X														2	12%
	5.2 Consciencialização da ameaça			X										X	X				3	18%
	5.3 Planos de ação e mecanismos de alerta					X		X					X				X	X	5	29%
Infraestruturas	6.1 Ausência de identificação de infraestruturas críticas					X									X		X		3	18%
	6.2 Estratégia e planos de resiliência de infraestruturas		X	X		X							X				X		5	29%
	6.3 Dependência Tecnológica					X		X					X				X		4	24%
Ciber e Espaço	7.1 Capacidade resposta a ciber ameaças				X									X	X				3	18%
	7.2 Estratégia espaço e resiliência ciber e digital	X	X	X	X	X		X				X	X	X	X		X		11	65%
	7.3 Dependência tecnológica e dimensão económica					X					X			X			X		4	24%
Cultural	8.1 Consciencialização da ameaça			X	X	X	X				X								5	29%
	8.2 Mecanismos de alerta e planos de ação					X											X		2	12%
	8.3 Capacidade económica		X					X			X			X			X		5	29%
Administração Pública	9.1 Reforma digital e estrutural	X	X		X	X	X			X	X	X	X	X	X		X		12	71%
	9.2 Consciencialização da ameaça			X				X											2	12%
	9.3 Falta de resiliência				X							X	X				X		4	24%
Legal	10.1 Ferramentas legais pouco eficazes	X	X			X					X		X	X			X	X	8	47%
	10.2 Consciencialização da ameaça			X	X	X					X		X					X	6	35%
	10.3 Sistema judicial moroso		X			X		X			X			X			X	X	7	41%
Social	11.1 Literacia social	X					X		X	X			X						5	29%
	11.2 Assimetrias sociais e demográficas		X			X		X	X		X		X	X					7	41%
	11.3 Consciencialização para segurança e ameaças			X	X	X									X				4	24%
Informações (Intel)	12.1 Falta cultura e capacidades Intel	X	X		X			X			X		X					X	7	41%
	12.2 Estratégia e resiliência Intel			X		X							X		X				4	24%
	12.3 Legislação deficiente para ação Intel					X										X			2	12%

Figura 11 – Unidades de registo e enumeração de vulnerabilidades

Apêndice H — Análises SWOT

1. Domínio Social

SWOT Domínio Social		Ambiente Interno	
		Potencialidades (P)	Vulnerabilidades (V)
		P1 - Unidade nacional e coesão social	V1 - Literacia social
		P2 - Garantia direitos fundamentais e proteção necessitados	V2 - Assimetrias sociais e demográficas
Ambiente Externo	Oportunidades (O)	Linhas de Ação Estratégica (LAE) que usam as Potencialidades para obter vantagens sobre as Oportunidades (PO)	LAE que usam as Oportunidades para superar as Vulnerabilidades (VO)
	O1 - Gestão de perceções e educação social		
	O2 - Comunicação estratégica	PO1 - Promover o apoio social e a necessitados.	VO1 - Desenvolver a Comunicação Estratégica.
	O3 - Conhecimento situacional	PO2 - Desenvolver os mecanismos gratuitos de saude, justica e educação.	VO2 - Elaborar plano de resiliência social .
	O4 - Estrutura de monitorização e identificação da ameaça e risco	PO3 - Criar equipas de apoio e suporte multidominio para apoio a entidades e civis	VO3 - Promover programa de educação/sensibilização governamental para uma estratégia governamental
	Ameaças (A)	LAE que usam as Potencialidades para evitar Ameaças (PA)	AE que minimizam as Vulnerabilidades para evitar Ameaças (VA
	A1 - Campanhas de desinformação e propaganda	PA1 - Reforçar a partilha da situação das ameaças com a NATO e UE.	VA1 - Promover a literacia digital.
		PA2 - Criar mecanismos legais para controlo da desinformação e propaganda.	VA2 - Criar mecanismos e processos de vigilância e alerta e coordenação do CAH.

Figura 12 – Análise SWOT no domínio Social

2. Domínio Infraestruturas

SWOT Domínio Infraestruturas		Ambiente Interno	
		Potencialidades (P)	Vulnerabilidades (V)
		P3 - Planos Resiliência Infraestruturas	3 - Falta Estratégia e planos de resiliência de infraestrutura
		P4 - Infraestruturas abastecimento espaço europeu	V4 - Dependência Tecnológica
Ambiente Externo	Oportunidades (O)	Linhas de Ação Estratégica (LAE) que usam as Potencialidades para obter vantagens sobre as Oportunidades (PO)	LAE que usam as Oportunidades para superar as Vulnerabilidades (VO)
	O5 - Estratégia de resiliência Ciber das Infraestruturas críticas	PO1 - Elaborar plano de resiliência em infraestruturas criticas.	VO1 - Fomentar a resiliência ciber das infraestruturas criticas com programas de desenvolvimento UE e
	O6 - Estrutura de monitorização e identificação da ameaça e risco	PO2 - Incrementar a captação de investimento e inovação em infraestruturas criticas.	VO2 - Promover planos de contigencia para infraestruturas criticas.
	O7 - Cooperação internacional NATO/UE	PO3 - Criar mecanismos e sistema de vigilância e alerta, interligados aos similares europeus e NATO.	VO3 - Incrementar estratégias de cooperação e parcerias económicas entre estado e privados.
	O8 - Conhecimento situacional		
	Ameaças (A)	LAE que usam as Potencialidades para evitar Ameaças (PA)	E que minimizam as Vulnerabilidades para evitar Ameaças (V
	A2 - Cyberespionagem	PA1 - Promover programas de afirmação de infraestruturas nacionais como portas de mercado com a UE	VA1 - Promover o investimento em industrias tecnologicas e digitais.
	A3 - Operações Cyber	PA2 - Elaborar plano de resiliência infraestruturas com objetivos de cibersegurança e contraespionagem.	VA2 - Criar mecanismos de certificação e validação em segurança de infraestruturas em coordenação com a UE.
		PA3 - Promover a resiliência da UE e da NATO, concorrendo e promovendo a resiliência de	VA3 - Reforço do papel da inovação e capital humano como factores catalisadores da cibersegurança nacional

Figura 13 – Análise SWOT no domínio Infraestruturas

3. Domínio Informacional

SWOT Domínio Informacional		Ambiente Interno	
		Potencialidades (P)	Vulnerabilidades (V)
		P5 - Pluralidade e confiança na informação	V5 - Falta Consciencialização da ameaça
		P6 - Diversidade plataformas eletrónicas de comunicação	V6 - Falta Planos de ação e mecanismos de alerta
Ambiente Externo	Oportunidades (O)	Linhas de Ação Estratégica (LAE) que usam as Potencialidades para obter vantagens sobre as Oportunidades (PO)	LAE que usam as Oportunidades para superar as Vulnerabilidades (VO)
	O9 - Conhecimento situacional	PO1 - Promover a independência e liberdade dos meios de comunicação.	VO1 - Desenvolver Comunicação Estratégica.
	O10 - Estrutura de monitorização e identificação da ameaça e risco	PO2 - Apoiar tecnologias disruptivas emergentes como IA e big data para vigilância e detetar desinformação.	VO2 - Elaborar plano de resiliência Informacional .
	Ameaças (A)	LAE que usam as Potencialidades para evitar Ameaças (PA)	LAE que minimizam as Vulnerabilidades para evitar Ameaças (VA)
	A4 - Controlo e influência do Media	PA1 - Reforçar a partilha da situação Informacional com a NATO e UE.	VA1 - Promover a informação da Ameaça e do Risco.
		PA2 - Criar mecanismos legais para evitar centralização e controlo dos media.	VA2 - Criar mecanismos e processos de vigilância e alerta e coordenação do CAH.
		PA3 - Promover mec de dissuação de ameaças híbridas através de ações punitivas em coordenação c/ UE e NATO.	VA3 - Promover capacidade de cbt à desinformação, através deteção precocemente e desmentidos rápidos e firmes.

Figura 14 – Análise SWOT no domínio Informacional

4. Domínio Económico

SWOT Domínio Económico		Ambiente Interno	
		Potencialidades (P)	Vulnerabilidades (V)
		P7 - Inovação e indústrias tecnológicas digitais e espaciais	V7 - Limitada competitividade económica e orçamental
		P8 - Espaço UE de trocas comerciais e progresso económic	V8 - Dependência externa especialmente em recursos ener
Ambiente Externo	Oportunidades (O)	Linhas de Ação Estratégica (LAE) que usam as Potencialidades para obter vantagens sobre as Oportunidades (PO)	LAE que usam as Oportunidades para superar as Vulnerabilidades (VO)
	O11 - Estratégia de resiliência económica em infraestruturas críticas	PO1 - Elaborar plano de resiliência económica em infraestruturas criticas.	VO1 - Fomentar a resiliência económica com programas de desenvolvimento europeus e parcerias económicas.
	O12 - Desenvolver indústria e planos de investimento	PO2 - Incrementar a captação de investimentos e inovação em industrias tecnológicas e digitais.	VO2 - Promover parcerias e investimentos preventivos estr
	O13 - Conhecimento Situacional	PO3 - Criar mecanismos e sistema de vigilância e alerta, interligados aos similares europeus e NATO.	VO3 - Incrementar estratégias de cooperação e parcerias económicas entre estado e privados.
	Ameaças (A)	LAE que usam as Potencialidades para evitar Ameaças (PA)	E que minimizam as Vulnerabilidades para evitar Ameaças (V
	A5 - Criar e explorar dependências económicas	PA1 - Mitigar de forma gradual a dependência de bens e serviços externos.	VA1 - Promover a diversificação de dependências energéticas através de mecanismos de cooperação
	A6 - Espionagem Industrial	PA2 - Elaborar plano de resiliência económico com objetivos de cibersegurança e contraespionagem.	VA2 - Criar mecanismos de certificação e validação em segurança ciber com apoio e coordenação com a UE.

Figura 15 – Análise SWOT no domínio Económico

5. Domínio Informações

SWOT Domínio Informações		Ambiente Interno	
		Potencialidades (P)	Vulnerabilidades (V)
		P9 - Sistema integrado de centralização Intel	V9 - Falta cultura e capacidades Intel
		P10 - Intercambio Intel com NATO e UE	V10 - Estratégia e resiliência Intel
Ambiente Externo	Oportunidades (O)	Linhas de Ação Estratégica (LAE) que usam as Potencialidades para obter vantagens sobre as Oportunidades (PO)	LAE que usam as Oportunidades para superar as Vulnerabilidades (VO)
	O14 - Cooperação internacional NATO/UE	PO1 - Elaborar plano de resiliência de Informações.	VO1 - Fomentar a melhoria de capacidades e recursos intel através da UE e NATO.
	O15 - Estratégia de resiliência em ciberdefesa	PO2 - Criar mecanismos de partilha de Informações e alerta com a UE e NATO.	VO2 - Promover as estratégias de resiliência ciber da UE e NATO para promover estratégia nacional de resiliência ciber.
		PO3 - Promover sistemas de procura e alerta, e mecanismos de integração e a cooperação interministrial.	VO3 - Promover a cooperação da UE e da NATO, concorrendo para respostas coordenadas à AH
	Ameaças (A)	LAE usam as Potencialidades evitar Ameaças (PA)	LAE minimizam as Vulnerabilidades evitar Ameaças (VA)
	A7 - Sistemas de Informações	PA1 - Reforçar a partilha de informações com a NATO e UE.	VA1 - Promover uma cultura e capacidade intel nacional e cooperante nos diversos dominios de seguranca.
	A8 - Operações Clandestinas	PA2 - Criar mecanismos de cooperação intel civil-militar.	VA2 - Criar mecanismos e processos de vigilância e alerta e coordenação do CAH.
		PA3 - Garantir a resiliência digital nacional	VA3 - Apoiar tecnologias disruptivas emergentes como IA e big data para vigilância
		PA4 - Adaptação dos exercícios nacionais injetando elementos hibridos nos exercicios e ligação civil-militar	VA4 - Criar mecanismos de cooperação ciber civil-militar para deter, defender e combater todo o espectro de ameaças cibernéticas.

Figura 16 – Análise SWOT no domínio Informações

Apêndice I — Objetivos e Linhas de Ação

Quadro 16 – Objetivos, LA e validação

Obj Est	LA	Classificação e Risco	Validação
Aumentar o Conhecimento Situacional	**LA 1 - Criar mecanismos de integração, de vigilância e alerta e coordenação interministerial de ameaças e riscos.**	**Adequação - Elevada:** Não apenas para este ObjEst, mas para com os outros, a LA1 é considerada altamente adequada na compreensão das ameaças ao Estado e à sociedade, e na preparação da primeira resposta de defesa e combate às ameaças híbridas. **Exequibilidade - Baixa:** Dada a falta de coordenação interna apresentada por alguns ministérios, salientada a dificuldade em criar mecanismos de coordenação, vigilância e alertas interministeriais. Necessidade de um *approach Top-Down*, em que o Governo (na pessoa do Senhor Primeiro-Ministro) reconheça a necessidade da contínua modernização, e reforma das estruturas ministeriais, decidindo em Conselho de Ministros a criação e manutenção de uma Comissão Interministerial para o efeito da LA1. Outros possíveis modelos de organização e talvez mais adequados, pelo maior impacto no ObjEst: A criação de uma Secretaria de Estado, transversal a todos os ministérios, dedicada à monitorização, coordenação, alerta e vigilância das diferentes ameaças. Esta é prática comum, em nações como Israel, onde se constituem Secretarias de Estado para coordenar ações interministeriais de combate a ameaças externas e internas. • **Aceitabilidade - Elevada:** A coordenação e partilha de informações interministeriais é vital para que se consiga identificar as múltiplas dimensões de uma ameaça que não é apenas de segurança interna, ou económica, ou de fuga de capitais, ou de saúde pública. Todas, numa só.	✓
	LA 2 - Reforçar a partilha de informação da situação das ameaças com a NATO e a UE e entre estas.	**Adequação - Elevada:** O combate eficaz às ameaças híbridas exige uma partilha contínua e oportuna de informações estratégicas com real valor político e militar. **Exequibilidade - Neutra:** Em termos de infraestrutura de comunicação seguras, a Rede BICES criou pontos de acesso às comunidades de J2 nacionais, que através de um MOU podem ser expandidas às agências da UE. O desafio (ou impedimento) à exequibilidade é político e não de recursos. Múltiplos documentos do Step 1 do NDPP reconhecem a necessidade da criação de novas capacidades (de natureza política) que vão para lá do mandato da NATO, e que exigem uma maior coordenação com a União Europeia. Os centros de excelência compartilhados (i.e. Hybrid COE), são resultado do compromisso político interorganizacional. • **Aceitabilidade - Elevada:** O Conhecimento Situacional deve ser 360º e por isso Político, Militar, Económico, Social, Informacional, e sobre Infraestruturas. Este conhecimento nasce da partilha de informações sobre as ameaças de diferentes dimensões e de uma coordenação próxima entre a NATO e as respetivas capacidades da UE. As ameaças híbridas exploram vulnerabilidades de diferentes dimensões, às quais nenhum estado-membro da NATO ou da EU, está isento, sendo necessária a harmonização e sincronização de informações.	✓
	LA 3 - Promover a informação publica e educação da sociedade no âmbito das ameaças e dos riscos, nomeadamente na educação da cidadania e educação governamental.	**Adequação - Elevada:** Um dos centros de gravidade das democracias encontra-se na sua sociedade. Pelo qual é necessário escuda-la através do esclarecimento público sobre ameaças coordenadas e de múltiplas dimensões, objetivando destabilizar o tecido socioeconómico para atingir fins políticos. Proteger *hearts and minds* requer que os governantes e líderes estejam também cientes da real dimensão das ameaças, e que as suas decisões sejam acima de tudo conscientes e informadas. **Exequibilidade - Elevada:** Existem todos os recursos necessários à execução da LA3. • **Aceitabilidade - Neutra:** Toda e qualquer forma de esclarecimento público tem reflexos sociais positivos e negativos. É importante tratar a educação da sociedade com respeito e cuidado, uma vez as democracias ocidentais são adversas a mecanismos políticos (e especialmente militares) de condução de comportamento social. Neste sentido, de forma a controlar a narrativa e evitar especulações sobre procedimentos internos de reeducação das massas ou formas de neo-propaganda política, é crucial encaixar estes programas em contextos comunitários.	✓
Reforçar a Comunicação estratégica	**LA 4 - Promover a Comunicação Estratégica no domínio Social e Informacional, em coordenação com o CoE Stratcom da NATO e a Divisão STRATCOM da EEAS.**	**Adequação - Elevada:** As tradicionais redes sociais são (ainda) lugar de disputa entre narrativas oficiais e especulativas. É necessário por isso uma grande transparência e sincronização entre a 'ação e a palavra'. **Exequibilidade - Neutra/Baixa:** Existe um problema de operacionalidade com o LA4. Este diz respeito à diminuição da participação das novas gerações (GenZ) nas 'clássicas' redes sociais. A curto prazo, o TTP adequado passa pela promoção nominal do STRATCOM em domínios sociais e informacionais de largo espectro; no entanto, a médio e longo prazo, é necessário estudar e atentar às novas tendências de comunicação, refletidas pelo contraditório comportamento antissocial dentro das redes sociais. É por isso essencial, não apenas promover, mas também modernizar a comunicação estratégica, os seus interlocutores, os veículos de emissão, e destinatários. • **Aceitabilidade - Elevada:** Se a promoção das comunicações estratégicas não estagnar no tempo e espaço, o custo justifica o resultado.	✓
	LA 5 - Promover a capacidade de combate à desinformação, através de deteção precocemente e desmentidos rápidos e firmes.	**Adequação - Elevada:** O combate contra campanhas de guerra híbrida tem normalmente maior sucesso quando iniciado durante a sua primeira fase – desinformação generalizada e controlo do ambiente das informações. A criação do *UE Counter Disinformation Task-Force*, tem provado a sua eficiência na proteção da opinião pública da União, no desmentir rápido e firme, e no controlo do ambiente das informações. **Exequibilidade - Neutra/Baixa:** Tal como o sucedido na LA1, Portugal tem todos os recursos para colocar em prática a LA5. No entanto como já se constatou, o Estado carece de interoperabilidade entre Ministérios e para incorporar uma capacidade estratégica desta dimensão, pode vir a necessitar de mandato ou no pior dos casos, escrutínio político. Em sistemas políticos como o Português, o desmentir rápido e firme requer grande coordenação entre ministérios e múltiplas confirmações políticas, que inevitavelmente poderão atrasar a resposta. • **Aceitabilidade - Elevada:** Para a defesa do Estado é necessário assegurar o controlo da narrativa, seja ela militar, política ou de outra dimensão. A aceitabilidade é total.	✓
Reforçar a Resiliência	**LA 6 - Criar equipas de apoio e resposta a ameaça multidomínio para apoio a entidades e civis**	**Adequação - Elevada:** As equipas de respostas são muitíssimo válidas uma vez que em caso de projeção de poder contra entidades civis ou indústrias nacionais, é necessário mover e implantar uma equipa de reação rápida para mitigar futuros impactos políticos, sociais, e económicos. O combate à ameaças híbridas não deve ser desvalorizado, ou colocado em paridade com o combate a ameaças CBRN. É necessário construir e equipar equipas civis-militares multidisciplinares com elementos especializados nas suas respetivas áreas. **Exequibilidade - Baixa:** Não existe prioridade governamental, não existe plano e não existe orçamento. • **Aceitabilidade - Elevada:** O sucesso ou insucesso no combate às ameaças híbridas depende muitas vezes da resiliência dos centros de gravidade e das primeiras linhas de defesa, nomeadamente no que diz respeito à proteção do tecido socioeconómico.	✓
	LA 7 - Criar mecanismos de certificação e validação em segurança ciber com apoio e coordenação com a UE.	**Adequação - Elevada:** A segurança de um é a segurança de todos. Torna-se assim uma prioridade garantir que as ciber capacidades do Estado Português cumpre os mais exigentes requisitos de segurança, e que estão certificadas pela UE. **Exequibilidade - Baixa:** Questões de soberania nacional, Segredo de Estado, protocolos de segurança e leis internas, impedem que toda a União mantenha o mesmo nível de ciber segurança. Ainda assim, para este efeito é possível impor um nível mínimo de segurança que pode ser auditado, validando um nível mínimo de cibersegurança europeu que deve ser atingido. • **Aceitabilidade - Neutra:** As limitações supracitadas podem limitar a aceitabilidade desta LA.	✓

	LA 8 - Promover coordenação e integração das estratégias de resiliência ciber da UE, NATO e a Estratégia Nacional de Segurança do Ciberespaço.	**Adequação - Elevada:** É adequado coordenar a Estratégia Nacional de Segurança no Ciberespaço com as melhores práticas Europeias e desenvolvidas no seio da NATO, Interoperabilidade é essencial para o sucesso das campanhas conjuntas multinacionais e por isso é necessário sincronizar as capacidades nacionais com as normas de estandardização em todas as dimensões DOTMLPFI. Por natureza específica e particular do domínio do ciberespaço, a vulnerabilidade técnica de uma nação pode comprometer o sucesso da UE ou NATO. Os objetivos de defesa nacional da estratégia de segurança do ciberespaço devem ter como mínimo denominador comum os mesmos vetores das políticas de defesa Aliada e objetivos da UE. As construções particulares às diferentes e mais variadas necessidades nacionais devem vir por acréscimo, uma vez que as políticas de defesa NATO refletem o estado-da-arte e as melhores práticas neste sector. **Exequibilidade - Baixa:** Desconhecimento estratégico político, desadequadas infraestruturas tecnológicas, e falta de priorização governamental, constituem os maiores impedimentos a esta LA. • **Aceitabilidade - Elevada:** Aceitabilidade total.	✓
	LA 9 - Reforço do papel da inovação e capital humano como fatores catalisadores da cibersegurança nacional.	• **Adequação - Elevada:** LA muitíssimo válida, uma vez que a inovação é a chave para o sucesso. • **Exequibilidade - Elevada:** Portugal tem todos os recursos necessários para treinar novas capacidades humanas no estado-da-arte da cibersegurança. Necessária visão e convergência política e estratégica para a condução de fundos para inovações sectoriais. • **Aceitabilidade - Elevada:** Este é um aspeto vital para o reforço da resiliência no ciberespaço.	✓
	LA 10 - Criar mecanismos legais de enquadramento do controlo da desinformação.	• **Adequação - Elevada:** LA 10 é francamente válida e essencial para a proteção dos direitos políticos e liberdades civis. É necessário introduzir nova legislação ou adaptar a lei à realidade do domínio fluído das informações. Sem um quadro legal e criminal bem definido, agentes externos e internos continuarão a explorar impunemente este ambiente. O trabalho do Centro de Investigação Jurídica do Ciberespaço, da Faculdade de Direito da Universidade de Lisboa, é um primeiro passo (académico) para reformar a lei do ciberespaço em Portugal. • **Exequibilidade - Elevada:** Embora existam capacidades técnicas e recursos humanos treinados para se executar esta LA é necessário um enquadramento estratégico nacional, que neste momento está ainda a dar os seus primeiros passos. • **Aceitabilidade - Elevada:** Aceitabilidade total.	✓
	LA 11 - Promover mecanismos de dissuasão de ameaças híbridas através de ações punitivas em coordenação com UE e NATO.	• **Adequação - Elevada:** Todos os mecanismos de dissuasão de ameaças híbridas devem ser empregues sempre que possível em coordenação com os membros parceiros da UE e NATO. • **Exequibilidade - Elevada:** Os estados Aliados e Estados-Membro da EU anunciaram várias vezes a necessidade de ação em bloco para contrariar estas projeções de poder. • **Aceitabilidade - Elevada:** Aceitabilidade Total.	✓
	LA 12 – Reforçar a coesão social, mantendo políticas de acesso gratuitos à saúde, à justiça e à educação e de apoio social e a necessitados.	• **Adequação - Baixa:** Embora uma estratégia válida, de todas as LA, é a que menos impacto terá no reforço da resiliência nacional. Este é um domínio de constante clivagem política, e que só deve ser considerado em casos extremos quando governos pretendem mudar drasticamente as suas políticas sociais, o que historicamente não acontece desde 1974. • **Exequibilidade - Neutra:** Esta LA pode comprometer as prioridades do Governo, mas está naturalmente dependente da particular agenda política do governo eleito. Poderão não existir recursos para manter o acesso universal e gratuito destes serviços aos cidadãos Portugueses, daí a expressão tendencialmente gratuito. • **Aceitabilidade - Neutra:** As oscilações das políticas sociais têm normalmente um impacto negativo na sociedade. A estabilidade social é um incremento positivo na resiliência nacional. Mas a coesão social não se limita ao livre acesso aos serviços básicos do estado.	✗
	LA 13 - Apoiar tecnologias disruptivas positivas emergentes como IA e *big data* para detetar desinformação e vigilância Intel.	• **Adequação - Elevada:** Esta LA é totalmente adequada ao reforço da resiliência nacional. Uma vez que as novas formas de projeção de poder são tão dispersas, é necessário a utilização de algoritmos (*deep-learning*) para monitorizar e detetar antecipadamente comportamentos erráticos no ciberespaço, potenciais ataques a sistemas críticos do Estado, ou campanhas de desinformação em massa. • **Exequibilidade - Baixa:** São necessários recursos e subsídios financeiros para que estas capacidades se desenvolvam, ou para captar a inteligência necessária para a criação de tecnologias de disrupção positiva. • **Aceitabilidade - Elevada:** Total, mas com necessidade de reformas legais.	✓
	LA 14 – Promover e incrementar a captação de investimento e inovação em infraestruturas críticas.	• **Adequação - Elevada:** A inovação é essencial e por isso é vital captar novo investimento... No entanto é crucial agir estrategicamente e de forma informada. É necessário reforçar o papel do GNS em Portugal, e de igual forma olhar para o modelo de investimento britânico e retirar lições - desenvolvimento de capacidades e infraestruturas críticas ficam a cargo das empresas com histórico nacional, credenciadas com as marcas apropriadas e debaixo do devido escrutínio dos auditores públicos. • **Exequibilidade - Elevada:** O único impedimento à exequibilidade desta LA é o reconhecimento público e político das vantagens e desvantagens da mesma. • **Aceitabilidade - Elevada:** Total.	✓
	LA 15 - Diversificar dependências energéticas através da promoção de parcerias e investimentos preventivos estratégicos e de mecanismos de cooperação europeus.	• **Adequação - Elevada:** A dependência energética é uma vulnerabilidade terrível com consequências políticas, sociais e económicas gravíssimas. Um país como Portugal (80% dependente de energia estrangeira), deve trabalhar para assegurar uma diversificação energética alargada, e trabalhar para explorar opções que permitam um dia sonhar com números de dependência abaixo dos 50%. Estados energeticamente independentes (como o caso da Noruega) apresentam políticas sociais mais firmes, estratégias de defesa nacional robustas, que contribuem naturalmente para um elevado orgulho patriótico, refletindo-se também numa sólida resiliência nacional. • **Exequibilidade - Baixa:** Numa política de defesa nacional, Portugal deve colaborar com os seus parceiros Europeus, mas também explorar reais oportunidades com os seus parceiros CPLP. A falta de recursos naturais (energéticos) em Portugal deveria potenciar o Governo Português para um maior investimento no I&D das energias. • **Aceitabilidade - Elevada:** Aceitabilidade total.	✓

	LA 16 - Incrementar estratégias de cooperação e parcerias económicas entre estado e privados.	• **Adequação - Elevada:** Desenvolvimento nacional advém de um sector privado saudável, cujo impacto do seu sucesso tem reflexos na sociedade nomeadamente através do índice de qualidade de vida. A resiliência nacional é normalmente mais forte em sociedades com um sector privado educado, treinado e financeiramente saudável. Parcerias entre Privados e entidades públicas não é apenas desejável, mas necessário para evitar estagnação dos processos. • **Exequibilidade - Neutra:** Os recursos existentes são suficientes para executar LA16, mas é necessária uma nova visão estratégica, com capacidades suficientes (não apenas financeiras) para captar o interesse dos privados. • **Aceitabilidade - Elevada:** Aceitabilidade total.	✓
	LA 17 - Incrementar a captação de investimento e inovação em indústrias tecnológicas e industriais.	• **Adequação - Baixa:** Embora seja reconhecidamente necessário participar na 4ª Revolução Industrial, o Governo Português não deve interferir com a autorregulação do mercado, mas promover o desenvolvimento do sector tecnológico através de futuras parcerias público-privadas, e patrocínio da indústria nacional nos mercados internacionais. • **Exequibilidade - Baixa:** A captação de investimento para uma determinada indústria não garante o seu sucesso. O Governo deve acompanhar as tendências do mercado no que diz respeito à oferta e à procura, apoiando determinados sectores de forma indireta. • **Aceitabilidade - Baixa:** A interferência do Estado na captação de investimentos numa indústria economicamente estagnada pode gerar vulnerabilidades no seio da resiliência nacional.	✗
	LA 18 - Promover uma cultura e capacidade Intel nos diversos domínios de segurança nacional, reforçando mecanismos de cooperação civil-militar.	• **Adequação - Elevada:** Embora Portugal não sofra de conflitos de jurisprudência interagências de segurança nacional, é necessário operacionaljzar respostas rápidas de forma a combater eficientemente as presentes ameaças híbridas. É absolutamente válido promover a partilha de *intelligence* entre as diferentes agências civis e militares responsáveis pela segurança e defesa da Nação. • **Exequibilidade - Neutra:** Para garantir uma partilha segura de intel entre agências é necessário capacitar as entidades civis com o mesmo nível de segurança da rede militar, treinar oficiais de segurança, e promover essa mesma cultura. • **Aceitabilidade - Elevada:** Aceitabilidade total, com grande impacto no combate inicial a ameaças híbridas.	✓
Reforçar a capacidade de prevenir e dar resposta a crises	**LA 19 - Elaborar plano de resiliência em infraestruturas critica com salvaguarda de cibersegurança e contraespionagem.**	• **Adequação - Elevada:** LA19 é desejável e necessária. Perfeitamente adequada às ameaças "*cíbridas*" que exploram as vulnerabilidades de sistemas SWET afetando em larga escala a estabilidade social e resiliência nacional. • **Exequibilidade - Elevada:** Para além dos recursos elementares para a preparação deste plano, é necessário contratar especialistas com experiência internacional no combate a ameaças "*cíbridas*", e não simplesmente do ciberespaço. A gramática de guerra é diferente e requer especialistas capacitados para enquadrar o plano com uma perspetiva estratégica. • **Aceitabilidade - Elevada:** Total.	✓
	LA 20 - Elaborar plano de resiliência económico.	• **Adequação - Elevada:** Esta LA é das mais importantes no combate às ameaças externas não lineares. • **Exequibilidade - Elevada:** Total. • **Aceitabilidade - Elevada:** A resiliência económica é um dos centros de gravidade das democracias ocidentais, e também um dos alvos mais vulneráveis. Durante uma campanha de guerra híbrida é necessário garantir o normal funcionamento da sociedade, apoiada numa economia funcional e escudada de futuros ataques.	✓
	LA 21 - Elaborar plano de resiliência de Informações.	• **Adequação - Elevada:** Portugal deve intervir junto dos seus parceiros NATO e UE, promovendo uma maior partilha de informações que possam ajudar a reforçar o conhecimento situacional, a natureza da ameaça multidimensional e fortificar a resiliência de informações nacionais. O "*Agreed Intelligence NATO*" é um modelo claramente falhado, que requer de reforma imediata. Esta, está politicamente pendente devido às assimetrias políticas entre estados Aliados, mas não membros da UE. Em território nacional é necessário repensar o mandato do SIRP, e o fortalecimento das informações estratégias militares. • **Exequibilidade - Elevada:** Dependente de iniciativa política. • **Aceitabilidade - Elevada:** Total.	✓
	LA 22 - Elaborar plano de resiliência Informacional.	• **Adequação - Elevada:** O domínio Informacional representa também ele um centro de gravidade importante e normalmente usado como veículo e destinatário de várias ameaças híbridas. É por isso muitíssimo válido elaborar um plano nacional de resiliência informacional, que objetive coordenar capacidades e meios humanos para assegurar o controlo da batalha da narrativa e combater propaganda e PSYOPS. • **Exequibilidade - Elevada:** Dependente de iniciativa política. • **Aceitabilidade - Elevada:** Total.	✓
	LA 23 – Planear e promover exercícios com elementos híbridos para treinar a resiliência.	• **Adequação - Elevada:** Na impossibilidade de criar exercícios nacionais dedicados às ameaças híbridas e condições de guerra não-linear, reforça-se o grande valor estratégico em operacionalizar exercícios com incidentes de elementos híbridos, que por natureza envolveriam elementos SOF e entidades civis, mas também toda a estrutura de C2 das FA. • **Exequibilidade - Elevada:** Embora existam recursos materiais para se executar a LA23, é necessário integrar / contratar (civis ou militares) especialistas em ameaças multidominio, com conhecimento do estado-da-arte e das melhores práticas internacionais - o que levanta um desafio para montar uma equipa de trabalho. • **Aceitabilidade - Elevada:** O exercício em si, é pouco para gerar reais capacidades. Associado ao exercício é necessário trabalho de desenho do cenário de guerra, construção dos "*threat networks*" associados e pré-treino antes do STARTEX. Após o ENDEX é necessário usar a teoria das lições aprendidas para capturar os reais impactos do exercício e promover o progresso e desenvolvimento da doutrina militar Portuguesa, nos seus diferentes ramos.	✓

Legenda: Critério de rejeição ≥ a 2 com coeficiente nulo ou baixo.

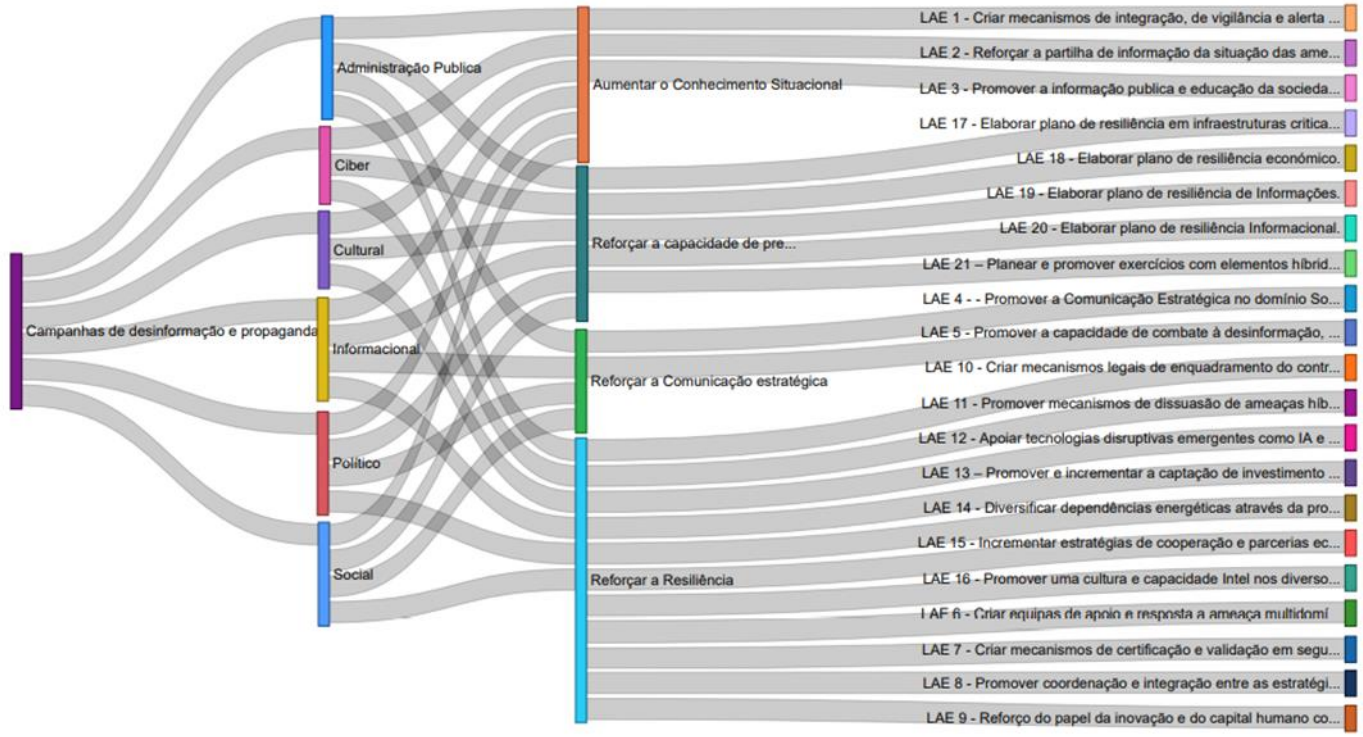

Figura 17 – PowerBI Campanhas de desinformação e propaganda

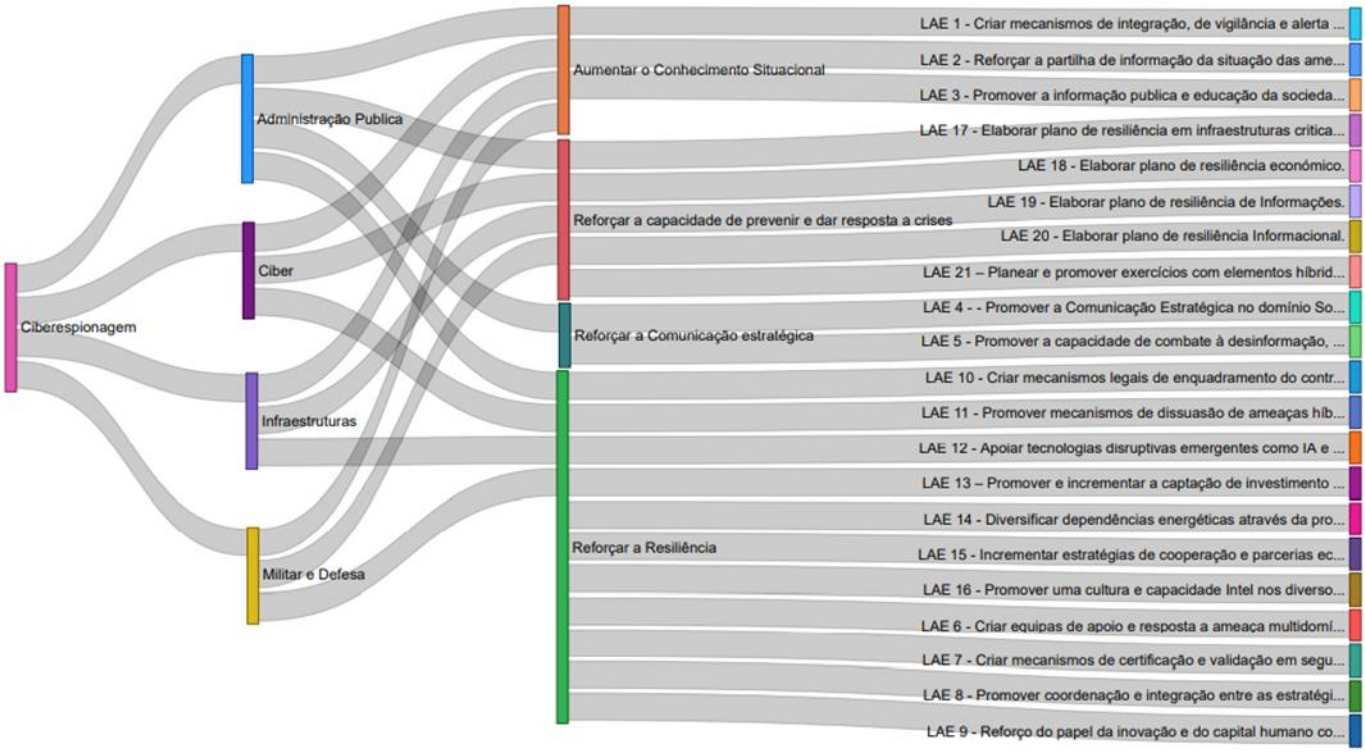

Figura 18 – PowerBI Ciberespionagem

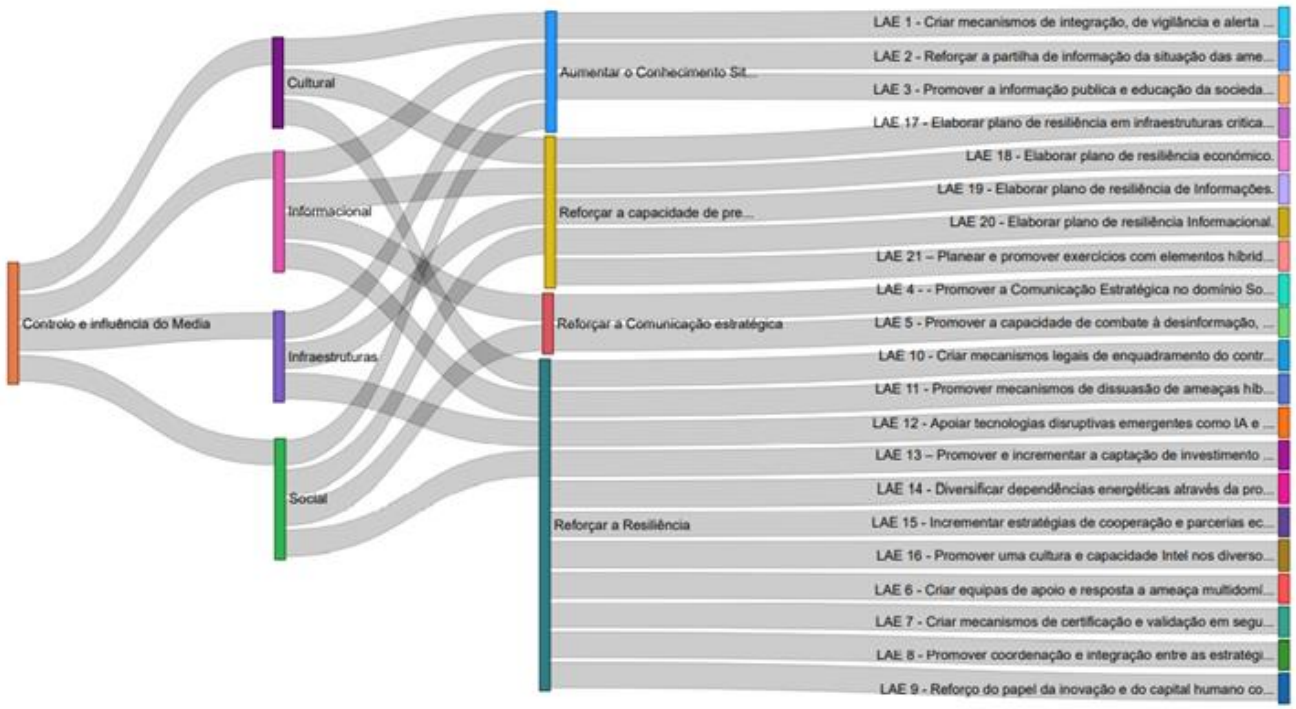

Figura 19 – PowerBI Controlo e influência do Media

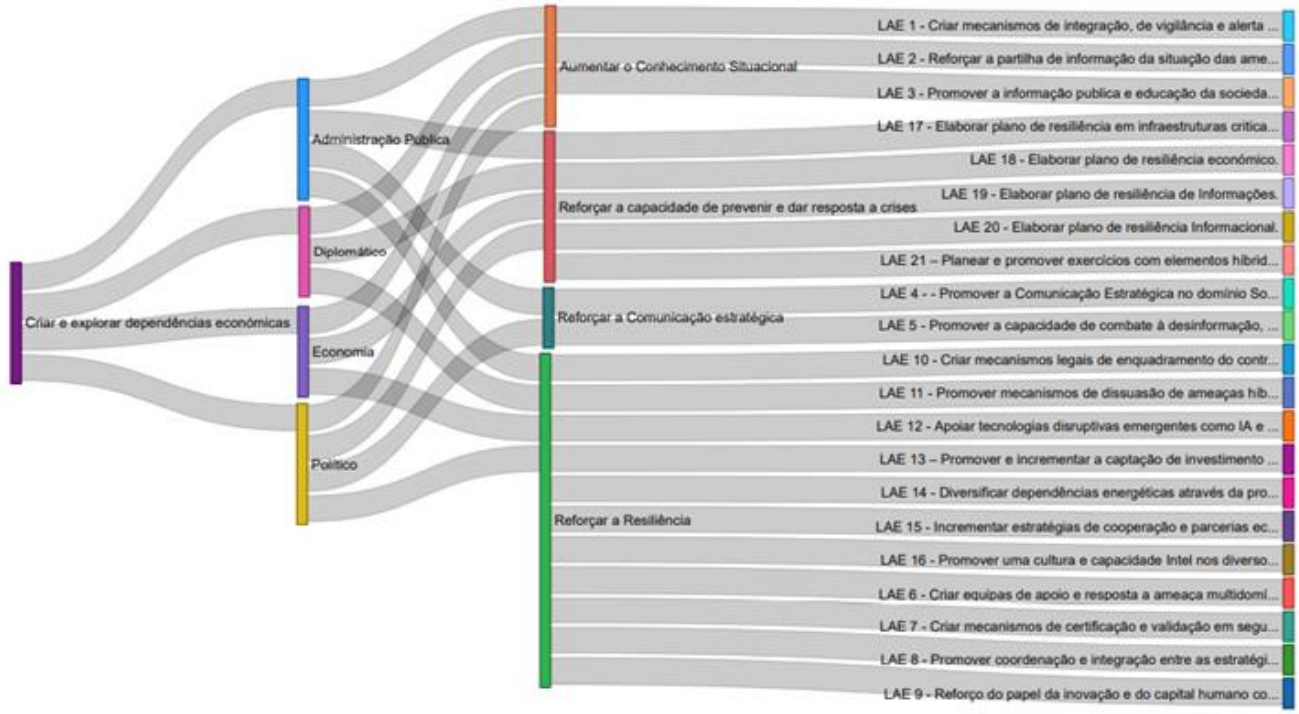

Figura 20 – PowerBI Criar e explorar dependências económicas

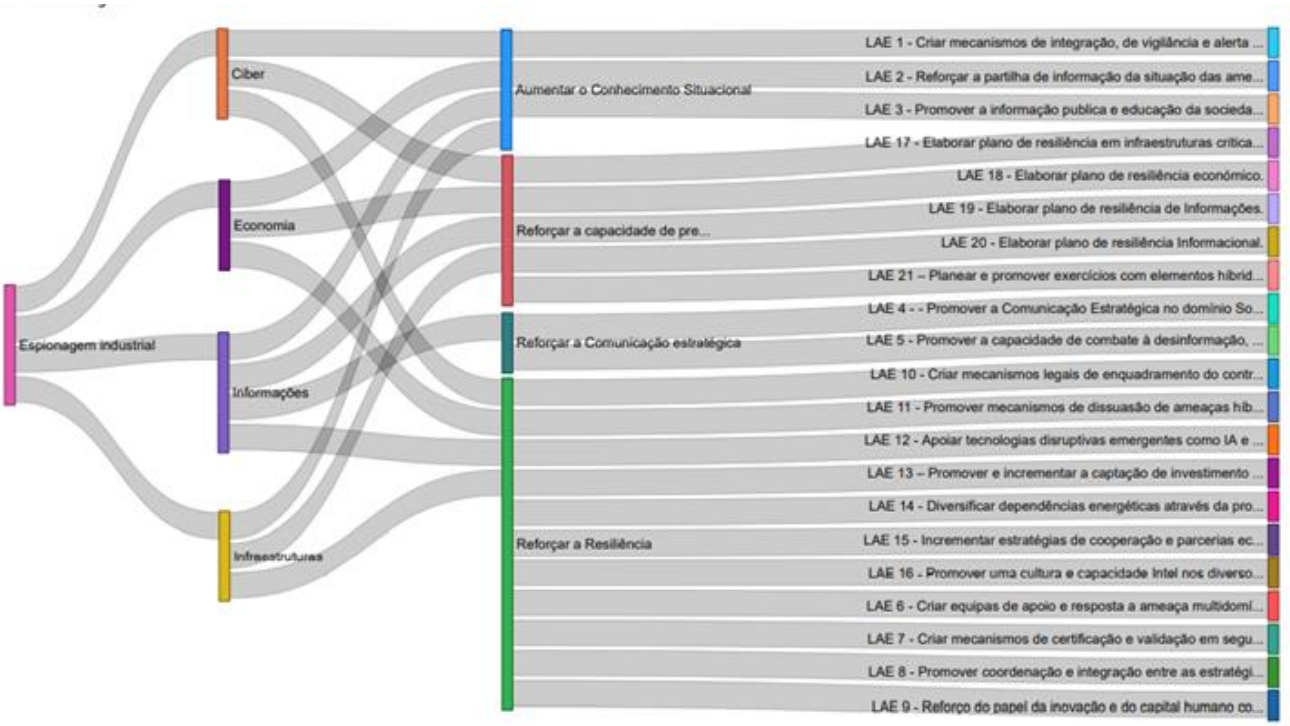

Figura 21 – PowerBi Espionagem industrial

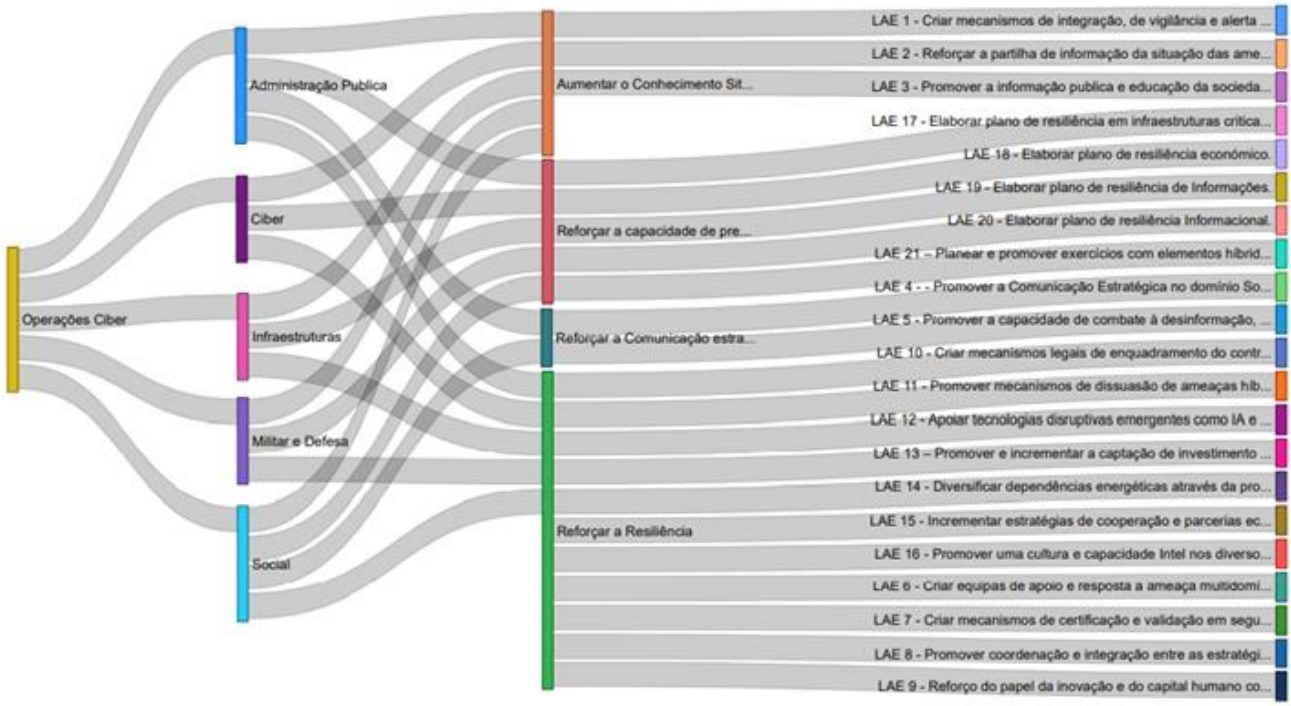

Figura 22 – PowerBI Operações Ciber

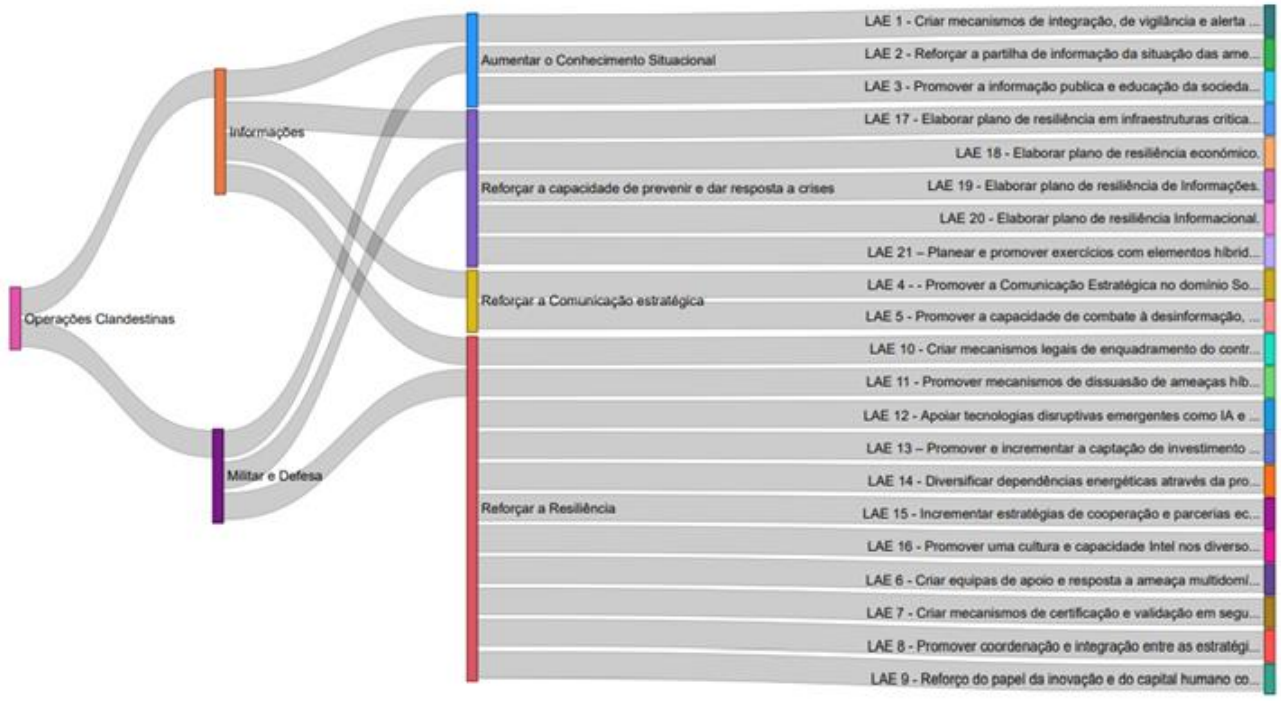

Figura 23 – PowerBi Operações clandestinas

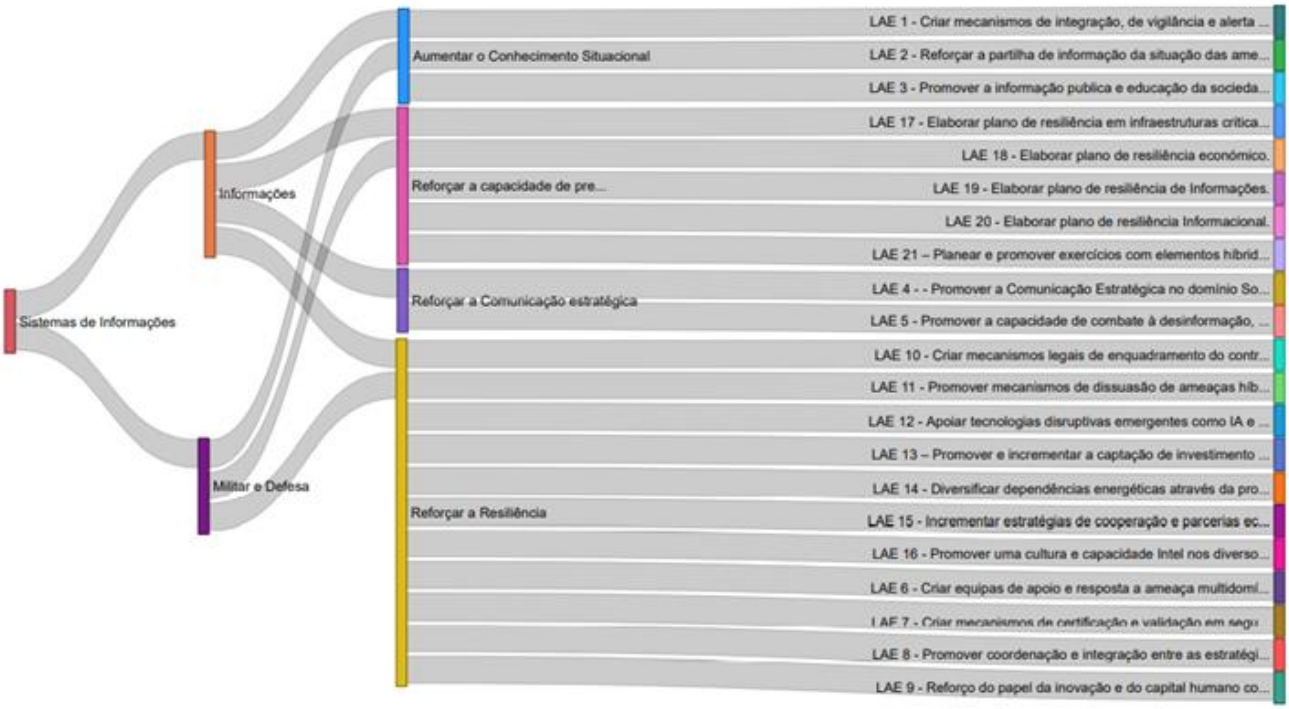

Figura 24 – PowerBI Sistemas de informações